Using Windows XP Professional with Service Pack 1 in a Managed Environment: Controlling Communication with the Internet

Microsoft Corporation

Published: January 2003

Table of Contents

Introduction 4
Activation and registration connected with a new installation or an upgrade 7
Application Help 11
Certificate support and the Update Root Certificates component 15
Device Manager 20
Driver Protection 23
Dynamic Update 27
Event Viewer 32
File association Web service 36
Help and Support Center: The Headlines and Online Search features 41
Internet Explorer 6 SP1 48
Internet games on Windows XP 54
Internet Information Services in Windows XP SP1 58
Internet Printing 61
Internet Protocol version 6 (IPv6) 65
MSN Explorer 72
NetMeeting 75
Online Device Help 88
Outlook Express 6 SP1 (included in Internet Explorer 6 SP1) 91
Plug and Play 96
Program Compatibility Wizard 100
Remote Assistance 104
Search Companion 109
Windows Error Reporting 112
Windows Media Player 122
Windows Messenger 135
Windows Time service 143
Windows Update and Automatic Update 155
Appendices 161
Appendix A: Resources for learning about automated installation and deployment 162
Appendix B: Resources for learning about Group Policy 166
Appendix C: Importing Group Policy settings for Windows XP to a server running Windows 2000 SP3 169
Appendix D: Application Compatibility Toolkit 171
Appendix E: Internet Connection Sharing and Internet Connection Firewall 174
Appendix F: Add Network Place Wizard 178
Appendix G: New Connection Wizard 180
Related Links 182

Introduction

Microsoft® Windows® XP Professional operating system includes a variety of technologies that communicate with the Internet to provide an improved user experience and robust features. Browser and e-mail technologies are obvious examples, but there are also technologies, such as Windows Update, that help users obtain the latest software and product information, including bug fixes and security patches. These technologies provide many benefits, but they also involve communication with Internet sites, which administrators might want to control.

Control of this communication can be achieved through a variety of options built into individual components, into the operating system as a whole, and into server components designed for managing configurations across your organization. For example, as an administrator you can use Group Policy to control the way some components communicate, or for some components, you can direct all communication to the organization's own internal Web site instead of an external site on the Internet.

This white paper provides information about the communication that flows between components in Windows XP Professional Service Pack 1 (SP1) and sites on the Internet, and how to limit, control, or prevent that communication in an organization with many users. The white paper is designed to help you, the administrator, plan strategies for deploying and maintaining Windows XP Professional SP1 in a way that provides an appropriate level of security for your organization's networked assets.

This white paper provides guidelines for controlling components in the following set of operating systems:

- Windows XP Professional SP1 on user computers. The focus is on the installation or configuration steps needed for these computers.

  Note This white paper does not cover desktop products other than Windows XP Professional SP1, for example, it does not cover Windows XP Home Edition or Windows XP Media Center Edition.

- Windows 2000 Service Pack 3 (SP3) on servers. The white paper does not focus on these computers, but it provides information for using these servers as part of your deployment or maintenance strategies. For instance, it describes ways of using Group Policy on a server running Windows 2000 SP3 to control the behavior or configuration of users' computers running Windows XP SP1.

The white paper is organized around individual components found in Windows XP Professional SP1, so that you can easily find detailed information for any component you are interested in.

What this white paper covers and what it does not cover

The subsections that follow describe:

- Types of components covered in this white paper
- Types of components not covered in this white paper
- Security basics that are beyond the scope of this white paper, with listings of some other sources of information about these security basics

Types of components covered in this white paper

This white paper provides:

- Information about components that in the normal course of operation send information to or receive information from one or more sites on the Internet. An example of this type of component is Windows Error Reporting; if a user chooses to use this component, it sends information to a site on the Internet.
- Information about components that routinely display buttons or links that make it easy for a user to initiate communication with one or more sites on the Internet. An example of this type of component is Event Viewer; if a user opens Event Viewer and clicks a link, the user is prompted with a message box that says, "Event Viewer will send the following information across the Internet. Is this OK?" If the user clicks OK, information about the event is sent to a Microsoft site, which replies with any additional information that might be available about that event.
- Brief descriptions of components like Microsoft Internet Explorer and Microsoft Outlook® Express that are designed to communicate with the Internet. It is beyond the scope of this white paper to describe all aspects of maintaining appropriate levels of security in an organization where users connect to sites on the Internet, download items from the Internet, send and receive e-mail, and perform similar actions. This white paper does, however, provide basic information about how Internet Explorer and Outlook Express work, and it provides suggestions for other sources of information about balancing users' requirements for access to the Internet with your organization's requirements for protection of networked assets.

Types of components not covered in this white paper

This white paper does not provide:

- Information about managing or working with applications, scripts, utilities, Web interfaces, Microsoft ActiveX® controls, extensible user interfaces, the .NET Framework, and application programming interfaces (APIs). These are either applications, or are layers that support applications, and as such provide extensions that go beyond the operating system itself. You must work with your software provider to learn what you can do to mitigate any risks that are part of using particular applications (including Web-based applications), scripts, utilities, and other software that runs on Windows XP SP1.
- Information about components that store local logs that could potentially be sent to someone or could potentially be made available to support personnel. This information is similar to any other type of information that can be sent through e-mail or across the Internet in other ways. You must work with your support staff to provide guidelines about the handling of logs and any other information you might want to protect.

Security basics that are beyond the scope of this white paper

This white paper is designed to help you, the administrator, plan strategies for deploying and maintaining Windows XP Professional SP1 in a way that provides an appropriate level of security for your organization's networked assets. The paper does not describe security basics, that is, strategies and risk-management methods that provide a foundation for security across your organization. It is assumed you are actively evaluating and studying these security basics as a standard part of network administration.

Some of the security basics that are a standard part of network administration include:

- Monitoring. This includes using a variety of software tools, including tools to assess which ports are open on servers and clients.
- Virus-protection software.
- The principle of least privilege (for example, not logging on as an administrator if logging on as a user is just as effective).

- The principle of running only the services and software that are necessary, that is, stopping unnecessary services and keeping computers (especially servers) free of unnecessary software.
- Strong passwords, that is, requiring all users and administrators to choose passwords that are not easily deciphered.
- Risk assessment as a basic element in creating and implementing security plans.
- Software deployment and maintenance routines to help ensure that your organization's software is running with the latest security updates and patches.
- Defense-in-depth. In this context, defense-in-depth (also referred to as in-depth defense) means redundancy in security systems, for example, using firewall settings together with Group Policy to control a particular type of communication with the Internet.

Other sources of information about security basics

The following books and Web sites are a few of the many sources of information about the security basics described previously:

- Howard, Michael, et al. *Designing Secure Web-Based Applications for Microsoft Windows 2000*. Redmond, WA: Microsoft Press, 2000.
- Howard, Michael, and David LeBlanc. *Writing Secure Code*. Redmond, WA: Microsoft Press, 2002.
- The Prescriptive Architecture Guides on the Microsoft Technet Web site at:

  www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/idc/pag/pag.asp

Activation and registration connected with a new installation or an upgrade

The following subsections provide information about:

- The purposes of activation and registration connected with a new installation or an upgrade
- How a user’s computer communicates with sites on the Internet during activation and registration
- Choosing volume licensing so that product activation need not take place (to limit the flow of information to and from Internet sites)

Purposes of activation and registration connected with a new installation or an upgrade

This subsection briefly describes the differences between product activation and registration, and then describes the purpose of each.

Product registration involves the provision of personally identifiable information, such as an e-mail address, to Microsoft for the purpose of receiving information about product updates and special offers. Registration is usually done on a per-product basis and is not required. If registration is completed, all registration information is stored using a variety of security technologies and is never loaned or sold outside Microsoft.

Product activation involves the authentication with Microsoft of non-personally identifiable information, including the product identifier for Microsoft Windows XP Professional Service Pack 1 (SP1) and a hardware hash representing the computer, for the purpose of reducing software piracy. (A hardware hash is a non-unique number generated from the computer's hardware configuration.) Activation of Windows XP is required in situations where the product is not purchased through a volume licensing program such as Microsoft Select License, Microsoft Enterprise Agreement, or Microsoft Open License. Many computer manufacturers can bypass activation on software preinstalled on a new computer by binding the software to the computer’s basic input/output system (BIOS). In this situation, no activation of that software is required. Detailed information about product activation can be found on the following Web site:

www.microsoft.com/piracy/basics/activation/

For more information about volume licensing, see "Choosing volume licensing so that individual product activation need not take place," later in this section.

Activation is aimed at reducing software piracy as well as ensuring that Microsoft customers are receiving the product quality that they expect. Activation means that a specific product key becomes associated with the computer (the hardware) it is installed on. After that happens, that product key cannot be used for activation on other computers (unless the owner is enrolled in a special program that permits additional activations, for example, a program through the Microsoft Developer Network [MSDN]).

Overview: Activation and registration in the context of a managed environment

Product activation is an anti-piracy technology designed to verify that software products have been legitimately licensed. If you have software re-imaging rights granted under a Microsoft volume license agreement, and if you obtained Windows XP Professional SP1 through a retail channel or preinstalled by the computer manufacturer, you can re-image it with Windows XP Professional SP1 licensed through one of the Microsoft volume licensing programs. With volume licensing, there is no need to perform product activation.

How a computer communicates with sites on the Internet during activation and registration

Windows XP SP1 can be activated through the Internet or by phone. When it is activated through the Internet, Windows XP SP1 communicates with Web sites as follows:

- **Specific information sent or received**: During activation of Windows XP SP1, the following information is sent to the activation server at Microsoft:

  - Request information, that is, information necessary for successfully establishing communication with the activation server.
  - Product key information in the form of the product ID, plus the product key itself.
  - A hardware hash (a non-unique number generated from the computer's hardware configuration). The hardware hash does not represent any personal information or anything about the software. It is based on the MD5 message-digest hash algorithm, and consists of a combination of partial MD5 hash values of various computer components. The hardware hash cannot be used to determine the make or model of the computer, nor can it be backward-calculated to determine the raw computer information.
  - Date and time.
  - The language being used on the system (so that any error message that is sent back can be in the correct language).
  - The operating system being activated (and the version number of the activation software).

  Depending on the owner's preference, the preceding information is either sent over the Internet to the activation system at Microsoft, or the product key information and hardware hash (combined into one number) are called in by phone.

- **Default setting and ability to disable**: Product activation can only be disabled by installing the operating system with software acquired through one of the Microsoft volume licensing programs. Product activation can be bypassed by many computer manufacturers by their binding the product to the computer's BIOS instead. In all other cases, product activation cannot be disabled.

- **Trigger and user notification**: When activation is required, the operating system provides a reminder each time a user logs on and at common intervals until the end of the activation grace period stated in the End-User License Agreement (thirty days is the typical grace period). With software acquired through one of the Microsoft volume licensing programs, there is no need for activation, and therefore there are no reminders that appear about activation.

- **Logging**: Entries that track the progress of activation and registration (for example, return codes and error codes) are logged into a text file, *systemroot*\setuplog.txt. This file can be used for troubleshooting if activation (or any part of Setup) fails. If the owner of Windows XP chooses to register the product, two entries are made in the same log. One entry records the country or region that was chosen for the operating system. A second entry records whether the owner chooses to have Microsoft (or the computer manufacturer) send information about product updates and special offers. No other registration data is logged.

- **Privacy, encryption, and storage for activation data**: User privacy was a paramount design goal in building the product activation technology. No personally identifiable information is collected as part of activation. The data is encrypted (HTTPS) during transmission, and is stored on servers located in controlled facilities at Microsoft. The data is accessible to a small number of server and program support personnel who oversee and maintain the activation servers and the product activation program.

  To review the Microsoft online privacy statement on activation, see the following Web site at:

  www.microsoft.com/piracy/basics/activation/apolicy.asp

- **Privacy, encryption, and storage for registration data**: Registration data, which contains information that the customer chooses to send to Microsoft, is encrypted (HTTPS) during transmission. It is stored in unencrypted form on servers located in controlled facilities and can be seen by customer service representatives and marketing personnel.

  To review the Microsoft online privacy statement on registration, see the following Web site at:

  www.microsoft.com/piracy/basics/activation/prvcyms.asp

- **Transmission protocol and port**: When Windows XP SP1 is activated through the Internet and a modem is not used, the first transmission uses HTTP through port 80 and goes to wpa.one.microsoft.com/ to check the HTTP response code. A response code of less than 500 indicates that a product activation server is available. (With a modem, there is only a check to see whether the modem can currently be used to make a connection to the Internet.) If the product activation server can be reached (or for a modem, if a connection to the Internet can be made), any activation or registration data that is sent uses HTTPS through port 443.

Activation improvements in Windows XP SP1

Microsoft has introduced additional technological measures in Service Pack 1 for Windows XP aimed at ensuring legally licensed customers receive the full benefits of owning their valid license. Some of the changes include:

- Product key validation during activation.
- The addition of a three-day grace period, where re-activation is required because of a significant hardware change. (Before Service Pack 1, there was no grace period for re-activation after a significant hardware change.)
- The ability for volume license customers to encrypt their volume license product key in unattended installations.

For more information about the changes to activation in SP1 for Windows XP, see the following pages on the Microsoft Web site at:

- www.microsoft.com/licensing/resources/vol/volkeys_winxpsp1.asp
- www.microsoft.com/piracy/basics/activation/windowsxpsp1.asp

Choosing volume licensing so that individual product activation need not take place

If you use the rights granted under a volume licensing agreement to purchase or re-image software, you cannot and need not perform activation on the individual computers that are installed under the volume license. Qualifying as a volume licensing customer is not difficult. Customers can qualify for the Microsoft

Open Licensing program by purchasing as few as five licenses. For more information, see the Microsoft licensing Web site at:

www.microsoft.com/licensing/

Application Help

The following sections provide information about:

- The benefits of Application Help
- How Application Help communicates with sites on the Internet
- How to control Application Help to prevent the flow of information to and from the Internet

Benefits and purposes of Application Help

Application Help is one of the application compatibility technologies that support the installation and operation of applications on Microsoft Windows XP Professional Service Pack 1 (SP1). Because some applications that work on earlier versions of Windows might not function properly on Windows XP SP1, the application compatibility technologies were developed to solve these potential problems and enable a better user experience.

Application Help is most commonly used to block low-level applications—such as antivirus and disk-access utilities—that were not written for or intended for use on Windows XP. By blocking the installation of these applications, this feature serves to avert serious problems that could compromise system integrity.

Overview: Using Application Help in a managed environment

Despite testing applications before you deploy Windows XP SP1, you may still have applications being used in your organization that can cause system instability.

Application Help is the last line of defense against users attempting to install incompatible applications, and it is invoked only in rare instances. When a user tries to run an application for which there is no compatibility fix, Application Help is invoked by default. Windows XP uses information in a local database to determine if a user is about to run an incompatible application. Compatibility fixes are contained in a database file named SYSMAIN.SDB. The warning information used when an application cannot be run successfully is contained in another database file, APPHELP.SDB. The operating system uses matching information in SYSMAIN.SDB, which in turn determines what messages to draw from APPHELP.SDB to block the operation of applications with known compatibility problems and to inform users about them. The list of incompatible applications is updated through Windows Update.

Application Help generates a message that is presented to the user when a problematic process is about to initiate. A dialog box appears that contains a brief message about the problem, with the severity indicated by an icon:

- If the icon is a yellow triangle with an exclamation mark, then the application is *not blocked*, which means that the user is still able to run the application.
- If the icon is a red stop sign, then the application is *blocked*, which means that the user cannot run the application.

The way these Application Help messages lead the user to interaction with the Internet is described in the following subsection.

While Application Help provides a valuable function, administrators in a highly managed environment might want to block the installation of applications that would automatically invoke Application Help, and thereby have a user access the Internet. You can create custom Application Help messages that redirect the user to an internal site for more information. This is described in greater detail in the subsection, "Controlling Application Help to prevent the flow of information to and from the Internet."

How Application Help communicates with sites on the Internet

In the Application Help dialog box, the user can click the Details button, in which case additional information is displayed in the Help and Support Center for Windows XP. The Help content comes from either Microsoft.com if the computer is online, or from a local HTML Help file.

The following list describes how interaction with the Internet takes place when Application Help is invoked:

- **Specific information sent or received**: Selecting the Details button provides the user with a page from Microsoft.com. The information that is displayed may provide a link to a non-Microsoft Web site, depending on the application. The URL provided for non-Microsoft Web sites is unique to each application. No information is sent to the Internet and the user is not uniquely identified.
- **Default and recommended settings**: Application Help is enabled by default. Recommended settings are presented in the following topic, "Controlling Application Help to prevent the flow of information to and from the Internet."
- **Triggers**: A user tries to run an application that is not compatible with Windows XP SP1.
- **User notification**: When the user selects the Details button there is no indication of whether the information is coming from an internal or external site.
- **Logging**: No events related to Application Help are logged.
- **Encryption**: No information from the client is sent to the Internet.
- **Privacy policy**: Application Help is covered by the same policy that covers Windows Update.
- **Transmission protocol and port**: The transmission protocol used is HTTP and the port is HTTP 80.
- **Ability to disable**: You can prevent Application Help from sending the user to the Internet by creating custom Application Help messages.

Controlling Application Help to prevent the flow of information to and from the Internet

You can block an application with known compatibility problems, such as antivirus programs. You can also create custom Application Help messages that describe the problem and redirect users to an intranet site rather than sending them to the Internet for more information. To do this you use the Compatibility Administrator tool which is part of the Application Compatibility Toolkit.

Included on the CD for Windows XP, the Application Compatibility Toolkit is a collection of tools and documents that can help you resolve application compatibility problems. Administrators can download the toolkit and have it automatically updated.

For more information about the Application Compatibility Toolkit, see Appendix D, "Application Compatibility Toolkit."

How creating custom Application Help messages can affect users and applications

The user experience with Application Help will not change if you block applications with known compatibility problems and create custom Application Help messages. The only difference will be that when users click the Details button they are sent to an internal site for more information instead of to the Internet. Not only can you prevent users from accessing the Internet in this way, but you can also avoid having users try to install incompatible applications.

Procedures for installing the Application Compatibility Toolkit and creating a custom Application Help message

Once you have downloaded the toolkit you can use the Compatibility Administrator tool to create custom Application Help messages and to block specific applications from running.

To install the Application Compatibility Toolkit

1. Load the CD for Windows XP, and then open the \Support\Tools folder.
2. Run **ACT20.EXE**. The installation program will provide a link to the location where you can download the toolkit.
3. Follow the installation instructions. Once you have installed the toolkit you can run the Compatibility Administration tool to make the changes you need.

   Note When you click the executable file ACT20.EXE, you will automatically be linked to the latest version of the toolkit. You can also download the toolkit from: www.microsoft.com/windowsxp/appexperience/

To create custom Application Help messages

1. Click **Start**, click **All Programs**, click **Windows Application Compatibility Toolkit**, and then click **Compatibility Administration Tool**.
2. In the console tree, click **Custom Databases**, and then click **New Database**.
3. On the toolbar, click **AppHelp**. The **Create a custom AppHelp message** dialog box appears.
4. Enter information as prompted in the dialog box.
5. Save the new database file.

   Note When you have completed your entries and saved the file, you can deploy your changes to multiple computers running Windows XP SP1. See "Deploying Compatibility Fixes," in Compatibility Administrator Help.

Related Links

For complete information about application compatibility resources, see:

www.microsoft.com/windowsxp/appexperience/default.asp

Certificate support and the Update Root Certificates component

The following subsections provide information about:

- The benefits of the certificate functionality built into Microsoft Windows XP Professional Service Pack 1 (SP1), including the benefits of Update Root Certificates
- How Update Root Certificates in Windows XP SP1 communicates with sites on the Internet
- How to control Update Root Certificates to limit the flow of information to and from the Internet

Benefits and purposes of the certificate functionality in Windows XP SP1

Certificates, and the public key infrastructure of which they are a part, support authentication and encrypted exchange of information on open networks, such as the Internet, extranets, and intranets. A certificate securely binds a public key to the entity that holds the corresponding private key. With certificates, host computers on the Internet no longer have to maintain a set of passwords for individual subjects who need to be authenticated as a prerequisite to access. Instead, the host merely establishes trust in a certification authority. The host can establish this trust through a certificate hierarchy that is ultimately based on a root certificate, that is, a certificate from an authority that is trusted without assurances from any other certification authority.

Examples of times that a certificate is used are when a user:

- Uses a browser to engage in a Secure Sockets Layer (SSL) session
- Accepts a certificate as part of installing software
- Accepts a certificate when receiving an encrypted or digitally signed e-mail message

When learning about public key infrastructure, it is important to learn not only about how certificates are issued, but how certificates are revoked, and how information about those revocations is made available to clients. This is because certificate revocation information is crucial for a user's application that is seeking to verify that a particular certificate is currently (not just formerly) considered trustworthy. Certificate revocation information is often stored in the form of a certificate revocation list, although this is not the only form it can take. Applications that have been presented with a certificate might contact a site on an intranet or the Internet for information not only about certification authorities, but also for certificate revocation information.

In an organization where clients run Microsoft Windows XP Professional and servers run Windows 2000 Server, Windows 2000 Advanced Server, or Windows 2000 Datacenter Server, you have a variety of options in the way certificates and certification revocation lists (or other forms of certificate revocation information) are handled. For more information about these options, see the references listed in the next subsection, "Overview: Using certificates components in a managed environment."

The Update Root Certificates component in Windows XP SP1 is designed to automatically check the list of trusted authorities on the Microsoft Windows Update Web site when this check is needed by a user's application. Specifically, if the application is presented with a certificate issued by a certification authority that is not directly trusted, the Update Root Certificates component (if present) will contact the Microsoft Windows Update Web site to see if Microsoft has added the certification authority to its list of trusted authorities. If the certification authority has been added to the Microsoft list of trusted authorities, its certificate will automatically be added to the trusted certificate store on the user's computer. Note that the

Update Root Certificates component is optional with Windows XP SP1, that is, it can be removed or excluded from installation on a computer running Windows XP SP1.

Overview: Using certificates components in a managed environment

In an organization where clients run Windows XP Professional and servers run Windows 2000 Server, Windows 2000 Advanced Server, or Windows 2000 Datacenter Server, you have a variety of options in the way certificates are handled. For example, you can establish a trusted root authority, also known as a root certification authority, that is inside your organization by using procedures in the documentation sources that follow. The first step in establishing a trusted root authority is to install the Certificate Services component. Another step that might be appropriate is to configure the publication of certificate revocation information to the Active Directory® directory service. When implementing public key infrastructure, it is recommended that you also learn about Group Policy as it applies to certificates.

When you configure a certification authority inside your organization, the certificates it issues can specify a location of your choosing for retrieval of additional evidence for validation. That location can be a Web server or a directory within your organization. Because it is beyond the scope of this paper to provide full details about working with certification authorities, root certificates, certificate revocation, and other aspects of public key infrastructure, see the following references for more information:

- "Troubleshooting Certificate Status and Revocation," a white paper on the Microsoft Technet Web site at:

  www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/WinXPPro/support/tshtcrl.asp

- Help for Windows 2000 Server, Windows 2000 Advanced Server, or Windows 2000 Datacenter Server.

  You can view the Windows 2000 Help on the Web at:

  www.microsoft.com/windows2000/techinfo/proddoc/

- The Windows 2000 Server Resource Kit, *Deployment Planning Guide* (especially the "Active Directory Infrastructure" chapter).

  You can view the Windows 2000 Resource Kits on the Windows Deployment and Resource Kits Web site at:

  www.microsoft.com/reskit/

In a medium-size to large organization, for the greatest control of communication with the Internet, it is recommended that you manage the list of certification authorities yourself, meaning that on users' computers, you would remove the Update Root Certificates component or prevent it from being installed with Windows XP SP1.

How Update Root Certificates communicates with sites on the Internet

This subsection focuses on how the Update Root Certificates component communicates with sites on the Internet. The previous subsection, "Overview: Using certificates components in a managed environment" provides references for the configuration choices that control the way other certificates components communicate with sites on the Internet.

If the Update Root Certificates component is installed on a user's computer, and the user's application is presented with a certificate issued by a root authority that is not directly trusted, the Update Root Certificates component communicates across the Internet as follows:

- **Specific information sent or received**: Update Root Certificates sends a request to the Windows Update Web site, asking for the current list of root certification authorities in the Microsoft Root Certificate Program. If the untrusted certificate is named in the list, Update Root Certificates obtains that certificate from Windows Update and places it in the trusted certificate store on the user's computer. No user authentication or unique user identification is used in this exchange.

  The Windows Update Web site is located at:

  windowsupdate.microsoft.com/

- **Default setting and ability to disable**: Update Root Certificates is installed by default in Windows XP SP1. You can remove or exclude this component from installation on users' computers.

- **Trigger and user notification**: Update Root Certificates is triggered when the user is presented with a certificate issued by a root authority that is not directly trusted. There is no user notification.

- **Logging**: Events containing information such as the following will be logged:

  For Event ID 7:
  ```
  Description: Successful auto update retrieval of third-party root
  list sequence number from: URL_for_Windows_Update_Web_Site
  ```

  For Event ID 8:
  ```
  Description: Failed auto update retrieval of third-party root
  list sequence number from: URL_for_Windows_Update_Web_Site
  with error: hex_error_value
  ```

- **Encryption, privacy, and storage**: When requests or certificates are sent to or from Update Root Certificates, no encryption is used. Information about Update Root Certificates activity is not stored on any Microsoft server. Because no unique user identification is used in this exchange, there is no information to which the issue of user privacy applies.

- **Transmission protocol and port**: The transmission protocol is HTTP and the port is 80.

Controlling the Update Root Certificates component to prevent the flow of information to and from the Internet

If you want to prevent the Update Root Certificates component in Windows XP SP1 from communicating automatically with the Microsoft Windows Update Web site, you can remove or exclude this component from installation on users' computers. You can do this during workstation deployment by using standard methods for unattended installation or remote installation. If you are using an answer file, the entry is as follows:

```
[Components]
Rootautoupdate = Off
```

How removing or excluding Update Root Certificates from users' computers can affect users and applications

If the user is presented with a certificate issued by a root authority that is not directly trusted, and the Update Root Certificates component is not installed on the user's computer, the user will be prevented from completing the action that required authentication. For example, the user might be prevented from installing software, viewing an encrypted or digitally signed e-mail message, or using a browser to engage in an SSL session.

If you choose to remove or exclude Update Root Certificates from users' computers, consider providing instructions that tell users what to do if they receive untrusted certificates. For example, you could instruct users to contact a particular department in your organization if they receive an untrusted certificate, and have that department work with the user to ensure that the user can accomplish what is needed, for example, engaging in an SSL session or reading an encrypted e-mail message.

Procedures for excluding or removing the Update Root Certificates component from an individual computer

The following procedures describe:

- How to use Control Panel to remove the Update Root Certificates component from an individual computer running Windows XP SP1.
- How to exclude the Update Root Certificates component during unattended installation of Windows XP SP1 by using an answer file.

To remove the Update Root Certificates component from an individual computer running Windows XP SP1

1. Click **Start**, and then either click **Control Panel**, or point to **Settings** and then click **Control Panel**.
2. Double-click **Add or Remove Programs**.
3. Click **Add/Remove Windows Components** (on the left).
4. Scroll down the list of components to Update Root Certificates, and make sure the check box for that component is cleared.
5. Follow the instructions to complete the Windows Components Wizard.

To exclude the Update Root Certificates component during unattended installation by using an answer file

1. Using the methods you prefer for unattended installation or remote installation, create an answer file. For more information about unattended and remote installation, see Appendix A, "Resources for learning about automated installation and deployment."
2. In the [Components] section of the answer file, include the following entry:

   Rootautoupdate = Off

Device Manager

The following sections provide information about:

- The benefits of Device Manager
- How Device Manager communicates with sites on the Internet
- How to control Device Manager to limit the flow of information to and from the Internet

Benefits and purposes of Device Manager

Device Manager provides users and administrators with information about how the hardware on their computers is installed and configured, and how the hardware interacts with the computer's applications. With Device Manager, administrators can update the drivers (or software) for hardware devices, modify hardware settings, and troubleshoot problems.

Overview: Using Device Manager in a managed environment

Administrators can access Device Manager through Administrative Tools\Computer Management. Users can access Device Manager through the Control Panel\System\Hardware tab to view information about the hardware installed on their computers, but they must have administrative credentials to modify or update hardware.

Administrators or users with administrative credentials will typically use Device Manager to check the status of hardware and to update device drivers. Administrators who have a thorough understanding of computer hardware might also use Device Manager's diagnostic features to resolve device conflicts and change resource settings.

Device Manager works in conjunction with Windows Update to deliver updated drivers for installed hardware devices. As an IT administrator in a highly managed environment you might want to block certain administrators from downloading drivers through Device Manager. You can do this by configuring Group Policy to disable Windows Update. If you disable Windows Update then Device Manager cannot communicate with the Internet. The following subsection provides details about how Device Manager interacts with the Internet.

How Device Manager communicates with sites on the Internet

Device Manager communicates with the Internet when an administrator uses it to update a driver by selecting a hardware device and clicking Update Driver on the Action menu. This activates the Hardware Update Wizard. The way Device Manager communicates with the Internet is based on its interaction with Windows Update through the Hardware Update Wizard; therefore much of the information in this subsection is the same as for Windows Update. Additional details are described as follows:

- **Specific information sent or received**: See the section "Windows Update and Automatic Update" in this white paper.
- **Default and recommended settings**: Device Manager is enabled by default. See the subsection "Controlling Device Manger to limit the flow of information to and from the Internet" for recommended settings.

- **Triggers**: Through Device Manager an administrator starts the Hardware Update Wizard, or adds new hardware to a computer.
- **User notification**: See “Windows Update and Automatic Update.”
- **Logging**: Errors that result from problems installing hardware devices without drivers are logged to the event log.
- **Encryption, access, privacy policy, transmission protocol, and port**: Please see “Windows Update and Automatic Update.”
- **Ability to disable**: You cannot disable Device Manager directly. You can, however, prevent interaction with the Internet through Device Manager by disabling Windows Update.

Controlling Device Manager to limit the flow of information to and from the Internet

You can prevent the Internet from being accessed through Device Manager by disabling Windows Update or configuring where computers search for drivers. You use Group Policy settings to perform both of these procedures. If you disable Windows Update, users will still be able to use Device Manager to view information about their hardware devices. For administrators to be able to update drivers there is the option for manually downloading driver updates from the Windows Update Catalog, whereby they can be distributed on your managed network as needed.

For more information about the Windows Update Catalog, see the Windows Update Web site at:

windowsupdate.microsoft.com/

Procedure for controlling how drivers are updated through Device Manager

For the procedure to disable Windows Update see the section “Windows Update and Automatic Update” in this white paper. The procedure to eliminate Windows Update as a driver search location using Group Policy is included here.

To disable Windows Update as a driver search location

1. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.
   For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for learning about Group Policy."
2. Click **User Configuration**, click **Administrative Templates**, and then click **System**.
3. In the details pane, double-click **Configure Driver Search Locations,** and then click **Enabled**.
4. Select **Don’t Search Windows Update**.

Driver Protection

The following sections provide information about:

- The benefits of Driver Protection
- How Driver Protection communicates with sites on the Internet
- How to control Driver Protection to limit the flow of information to and from the Internet

Benefits and purposes of Driver Protection

The Driver Protection feature in Microsoft Windows XP Professional Service Pack 1 (SP1) prevents the operating system from loading drivers that are known to cause stability problems (for example, preventing Windows XP from booting). These drivers are listed in a Driver Protection List database included with Windows XP. Driver Protection checks this database during Windows operating system upgrades and at run time after the operating system is installed. These checks are performed to determine whether to load a driver under Windows XP.

Driver Protection also displays up-to-date content about these driver problems in Help and Support Center, including links where users can find a solution. Driver Protection relies on Windows Update and Dynamic Update to update the database files so that users are presented with the most current information available on protected drivers. Users cannot directly disable Driver Protection.

Drivers are added to the Driver Protection List based on feedback from end users about problems that can be reproduced and confirmed at Microsoft. The main reasons a driver is added to this list are:

- Windows XP cannot boot with this driver loaded.
- Windows XP Setup cannot complete with this driver loaded.
- End users experience data corruption when this driver is loaded under Windows XP.

Decisions to add drivers to this list are made in consultation with the vendors who produce and distribute these drivers. Microsoft engages and informs these vendors before adding a driver to the Driver Protection List.

A listing of the content in the Driver Protection List for Windows XP is available as part of a white paper that provides additional information about Driver Protection on the following site at:

www.microsoft.com/hwdev/driver/drv_protect.asp

This section of the white paper explains how to control Driver Protection in a managed environment.

Overview: Using Driver Protection in a managed environment

Users have no direct control over whether to download files required by Driver Protection for updating the Driver Protection List. In a managed environment it is unlikely that users will be allowed unlimited access to send and receive driver information; this function would normally be controlled in some fashion by the IT department. You can block Driver Protection’s ability to download files indirectly by disabling Windows Update or by avoiding the use of Dynamic Update. Details on the methods and procedures for controlling Driver Protection are described in the following subsections.

How Driver Protection communicates with sites on the Internet

This subsection summarizes the communication process:

- **Specific information sent or received**: No information is sent to the Internet about the user's system. Driver Protection downloads updated versions of the following files:
  - drvmain.sdb, apphelp.chm, apphelp.sdb, and apphelp.dll.
- **Default and recommended settings**: Driver Protection is enabled by default. Recommended settings are described in the next subsection, "Controlling Driver Protection to limit the flow of information to and from the Internet."
- **Triggers**: Driver Protection is triggered if the device driver is on the Driver Protection List when Windows XP starts, when a new application or device is installed, or during the installation or upgrade of the operating system.
- **User notification**: The notification that the user receives when Driver Protection is triggered differs according to when the driver load request occurs:
  - If a driver on the Driver Protection List is matched when Windows XP starts, the operating system displays a pop-up Help balloon titled "Devices or Applications disabled" in the taskbar notification area when the user logs on. If the user clicks that Help balloon, additional driver information and links to solutions for that problem are displayed in Help and Support Center.
  - If a driver on the Driver Protection List is matched during Windows XP Setup (for an upgrade from Windows NT® 4.0 or Windows 2000), a message will appear in the Report System Compatibility window before the operating system upgrade is completed.
    Users have two options at this point:
    - They can cancel Windows XP Setup and find an alternate driver solution before installing the new operating system. If the driver that users install solves the problem, Windows XP Setup will continue normally.
    - They can continue the upgrade process without first installing a driver that solves the problem. In this case, Setup may disable the driver in order to be completed. When users later log on, the operating system displays the pop-up Help balloon described in the previous case.

    If a driver on the Driver Protection List is matched during installation of a new application or device, and that driver uses system installation services (SetupAPI), the operating system displays a notification during installation and blocks the installation of that driver.

    If a driver is not installed using system installation services, Windows XP cannot block the installation of that driver. It can, however, block the driver from loading. If the driver is blocked, a notification will appear every time the operating system attempts to load that driver under Windows XP. For example, if a CD writing program that does not use system installation services installs a driver that is included on the Driver Protection List, Windows XP will display the pop-up Help balloon mentioned previously after the setup for that program is completed.
- **Logging**: If Driver Protection finds a match for a driver in the Driver Protection List, Windows XP logs an event in the event log.
- **Encryption**: The data packages downloaded to the user's system by Microsoft are digitally signed.
- **Access**: No data is uploaded from the user's computer.
- **Privacy policy**: Driver Protection is covered by the same policy that covers Windows Update.
- **Transmission protocol and port**: The transmission protocol used is HTTP and the port is 80.
- **Ability to disable**: You cannot disable Driver Protection directly. Disabling Windows Update or avoiding the use of Dynamic Update will, however, block Driver Protection from updating the database

files for the Driver Protection List on the user’s system. (Of course you can also disable Driver Protection by preventing access to the Internet, or by blocking HTTP over port 80.)

Controlling Driver Protection to limit the flow of information to and from the Internet

You cannot disable Driver Protection directly. To block Driver Protection, disable the settings for Windows Update and (during Setup) avoid the use of Dynamic Update. You can also block HTTP port 80 at the firewall or configure the Services snap-in. The following table describes the result of each option.

Configuration settings for Driver Protection

Configuration tool	Setting	Result
Windows Update	Block Windows Update. See the section titled "Windows Update and Automatic Update" in this white paper.	Blocks Driver Protection.
Dynamic Update	Avoid the use of Dynamic Update. See the section titled "Dynamic Update" in this white paper.	Blocks Driver Protection.
Firewall	Block HTTP port 80.	Blocks Driver Protection.
Services snap-in	Disable the Upload Manager service (uploadmgr).	Blocks Driver Protection. Any other services that depend on uploadmgr will also fail to start.

How controlling Driver Protection can affect users and applications

Driver Protection blocks known problem drivers from loading, but it does not block any associated applications that depend on those drivers. Therefore, the behavior of applications that depend on blocked drivers varies depending on the implementation of the application. Some applications, such as antivirus programs, install drivers in order to provide their core functionality. For these applications, Driver Protection may cause the application not to work at all. Other applications, such as CD-burning programs, use drivers for portions of their feature set. For these applications, only those features that do not depend on the driver may work.

If you decide to disable Driver Protection’s ability to pull down updated versions of the Driver Protection List database, drivers that affect system stability will continue to be blocked. The operating system, however, will use the version of the Driver Protection List database that comes with the operating system to identify the drivers to block, instead of a more accurate, up-to-date version of the list.

Alternate methods for controlling Driver Protection

A more drastic measure to take would be to disable the Upload Manager service (uploadmgr) that manages synchronous and asynchronous file transfers between clients and servers on the network. Disabling this service will block the upload of the anonymous hardware profile data (although users will still be able to complete the Hardware Wizard). The operating system will, however, use the version of the Driver Protection List database that comes with the operating system to identify the drivers to block, instead of a more accurate, up-to-date version of the list. The following subsection gives the procedure for this method.

Procedures for disabling how Driver Protection communicates over the Internet

You cannot disable Driver Protection directly but can do so indirectly by controlling its ability to connect to the Internet by disabling Windows Update or avoiding the use of Dynamic Update. See the sections in this white paper titled "Windows Update and Automatic Update" and "Dynamic Update" for more information about these methods.

As mentioned in the previous subsection, a more drastic method for disabling Driver Protection is to disable the Upload Manager service.

To disable how Driver Protection communicates over the Internet by disabling the Upload Manager service

1. Click **Start**, and then either click **Control Panel**, or point to **Settings** and then click **Control Panel**. Double-click **Administrative Tools**, and then double-click **Services**.
2. In the details pane, right-click **Upload Manager**, and then click **Properties**.
3. Click the **Log On** tab, then click the hardware profile that you want to configure, and then click **Disable**.

Important If this service is disabled, any services that explicitly depend on it will fail to start.

Related Links

For more information about Driver Protection in Windows XP, see the Microsoft Web site at:

www.microsoft.com/hwdev/driver/drv_protect.asp

Dynamic Update

The following subsections provide information about:

- The benefits of Dynamic Update
- How Dynamic Update communicates with sites on the Internet
- How to control Dynamic Update to limit the flow of information to and from the Internet

Benefits and purposes of Dynamic Update

With Dynamic Update, Windows XP Setup can check the Windows Update Web site for new Setup files, including drivers and other files, while Windows XP is being installed. In an interactive installation (in contrast to an unattended installation), the person installing Microsoft Windows XP Professional Service Pack 1 (SP1) chooses whether to allow Dynamic Update to occur.

In a managed environment, if you are using Winnt32.exe for unattended installation, you can create a shared folder on a server and deliver Dynamic Update files to destination computers from that shared folder (instead of downloading the files directly from the Windows Update Web site to the computer being installed). For additional information about how to do this, see "How Dynamic Update communicates with sites on the Internet" and "Controlling Dynamic Update to limit the flow of information to and from the Internet" later in this section.

Whenever an important update is made to any crucial Setup file, that update is made available through Dynamic Update functionality built into the Windows Update Web site. Some of the updated files will be replacements (for example, an updated Setup file) and some will be additions (for example, a driver not available at the time that the Setup CD was created). All files on the Dynamic Update section of the Windows Update Web site are carefully tested, and only files that are important in ensuring that Setup runs well are made available.

Dynamic Update decreases the need to apply patches to recently installed systems, and makes it easier to run Setup with hardware that requires a driver that was recently added or updated on Windows Update. For example, if a new video adapter requires a driver that was recently added to Windows Update, with Dynamic Update, the video adapter is recognized and supported during Setup.

Dynamic Update downloads only the files that are required for a particular computer, which means that the Dynamic Update software briefly examines the computer hardware. No personal information is collected, and no information is saved. The only purpose for examining the hardware is to select appropriate drivers for it. This keeps the download as short as possible and ensures that only necessary drivers are downloaded to the hard disk.

Overview: Using Dynamic Update in a managed environment

If you do not want Dynamic Update to connect to the Windows Update Web site during the installation of Windows XP, you have several options:

- **Creating a shared folder on a server and delivering Dynamic Update files to destination computers from that shared folder**: You can create a shared folder on a server in your organization, download Dynamic Update files to that server, and by using Winnt32.exe for unattended installations, ensure that when Setup for Windows XP SP1 is run in your organization, Dynamic Update uses the files you placed on the server and does not connect to the Internet.

- **Avoiding Dynamic Update**: You can avoid using Dynamic Update, which means Setup will use only the files and drivers provided on the CD for Windows XP SP1. For more information, see "Avoiding Dynamic Update" later in this section.

The subsections that follow provide more information about these options.

For additional sources of information about performing unattended installations, see Appendix A, "Resources for learning about automated installation and deployment."

How Dynamic Update communicates with sites on the Internet

This subsection focuses on the communication that occurs between Dynamic Update and the Windows Update Web site during an interactive installation (or a preinstallation compatibility check) when the computer has access to the Internet. This subsection also provides some description of the default behavior with unattended Setup.

For information about how you can control the behavior of Dynamic Update during unattended installations, see "Controlling Dynamic Update to limit the flow of information to and from the Internet" later in this section.

- **Specific information sent or received**: When Dynamic Update contacts the Windows Update Web site, it sends only the information necessary for appropriate drivers to be selected. In other words, it collects only necessary information about the hardware (devices) on that particular computer. No personal information is collected.

  The Setup files and drivers downloaded by Dynamic Update consist only of files that are important in ensuring that Setup runs successfully. Files with minor updates that will not significantly affect Setup are not made available through the Dynamic Update section of the Windows Update Web site. Some of the updated files will be replacements (for example, an updated Setup file) and some will be additions (for example, a driver not available at the time that the Setup CD was created).

- **Default behavior and triggers**:

  Dynamic Update connects to the Internet when Setup is run in certain ways. The following table provides details.

Choices for Setup and resulting Dynamic Update behavior in relation to the Internet

Action	Action details and results	Does Dynamic Update connect to the Internet?
Running a preinstallation compatibility check	Insert the Setup CD and choose the appropriate options for checking system compatibility. You are offered the choice of running or skipping Dynamic Update.	Yes, if you choose to run Dynamic Update.
Interactive installation	Start Setup from the CD or a network and run it interactively. You are offered the choice of running or skipping Dynamic Update.	Yes, if you choose to run Dynamic Update.
Unattended Setup without an answer file and without the use of any options that affect Dynamic Update	Run the Winnt32.exe command with the **/unattend** option, but do not provide the name of an answer file and do not specify **/DUdisable** or any other options that affect Dynamic Update. Dynamic Update is triggered under these conditions for both unattended installation and unattended upgrade.	Yes.
Unattended Setup with the **/DUdisable** option	Run the Winnt32.exe command with the **/unattend** option and also with the **/DUdisable** option. If the **/DUdisable** option is used, Dynamic Update is not triggered, regardless of whether	No.

	an answer file is used.	
Unattended Setup with an answer file that specifies that Dynamic Update should not be disabled	Create an answer file that includes an **[Unattended]** section with an entry that specifies **DUDisable = No**. Run the Winnt32.exe command with the **/unattend:***answer_file* option. Dynamic Update is triggered (but see the previous entry in this table).	Yes.
Unattended Setup with an answer file that does not specify any options that affect Dynamic Update	Run the Winnt32.exe command with the **/unattend:***answer_file* option. By default, if the answer file does not specify any options that affect Dynamic Update, Dynamic Update is disabled.	No.
Unattended Setup without an answer file and with the /DUShare option	Prepare a shared folder as outlined in "Creating a shared folder on a server and delivering Dynamic Update files to destination computers from that shared folder" later in this section. When you run Winnt32.exe, run it with the /**DUShare =** *path_to_downloaded_files* option. Dynamic Update uses the folder specified in the /DUShare option and does not connect to the Internet.	No, Dynamic Update uses the files in the shared folder that you created.
Unattended Setup with an answer file that contains the DUShare entry	Prepare a shared folder as outlined in "Creating a shared folder on a server and delivering Dynamic Update files to destination computers from that shared folder" later in this section. Create an answer file that includes an **[Unattended]** section with an entry that specifies **DUShare =** *path_to_downloaded_files*. Run the Winnt32.exe command with the **/unattend:***answer_file* option. Dynamic Update uses the folder specified in the DUShare entry and does not connect to the Internet.	No, Dynamic Update uses the files in the shared folder that you created.

- **User notification**: During an interactive installation, the user is notified when the choice of whether to run Dynamic Update is offered. During an unattended installation, there is no notification (unattended installation by definition means that no user interaction is required).

- **Logging**: By default, the progress of Setup is logged in *systemroot*\Winnt32.log. By using command options for the Winnt32.exe command, you can control the name of the log and the level of detail it contains.

- **Encryption**: The data is transferred from Microsoft using HTTP.

- **Access**: No information about the hardware (devices) on a particular computer is saved or stored, so no one can access this information. The information is used only to select appropriate drivers.

- **Privacy policy**: Dynamic Update is covered by the same policy that covers Windows Update. To view the privacy policy for Windows Update, see the Windows Update Web site, click **About Windows Update**, and scroll down until you see the heading "Windows Update Privacy Statement." The Windows Update Web site is located at:

  windowsupdate.microsoft.com/

- **Transmission protocol and port**: The transmission protocol is HTTP and the port is 80.

- **Ability to disable**: You can control the behavior of Dynamic Update by running Setup in specific ways, as shown in the table earlier in this subsection. (Of course you can also disable Dynamic Update by preventing access to the Internet, or by blocking HTTP over port 80.)

  If you do not want to disable Dynamic Update but only want to prevent it from communicating with an Internet site, as noted earlier, you can create a shared folder on a server and deliver Dynamic Update files to destination computers from that shared folder.

Controlling Dynamic Update to limit the flow of information to and from the Internet

As summarized in "Overview: Using Dynamic Update in a managed environment" earlier in this section, if you do not want Dynamic Update to connect to the Windows Update Web site during the installation of Windows XP, you have several options. With the appropriate methods for unattended installation, you can create a shared folder on a server and deliver Dynamic Update files to destination computers from that shared folder. Another alternative is to avoid using Dynamic Update at all.

Creating a shared folder on a server and delivering Dynamic Update files to destination computers from that shared folder

This subsection briefly describes the steps for creating a shared folder on a server and delivering Dynamic Update files to destination computers from that shared folder. The subsection also provides links to more detailed information. The steps can be summarized as follows:

- Step 1: Determine what packages you need to download from the Windows Update Web site.
- Step 2: Download the packages and prepare them and the folder they are in for use with Dynamic Update. This step includes extracting files and placing them in folders, as well as running the **/duprepare** option with Winnt32.exe, which creates subfolders and copies appropriate files to those subfolders. This step also requires other actions, such as sharing the folder and setting permissions.
- Step 3: Configure the answer file and Winnt32.exe settings for Dynamic Update (and for any other configuration options you want).
- Step 4: Run the unattended installations.

For more detailed information, see the *Windows XP Professional Resource Kit*, specifically Chapter 2, "Automating and Customizing Installations," especially the Dynamic Update information under the overview in that chapter. To view this chapter, see the TechNet Web site at:

www.microsoft.com/technet/prodtechnol/winxppro/reskit/prbc_cai_nmip.asp

Similar information is available in the Dynamic Update article on the Microsoft Web site at:

www.download.windowsupdate.com/msdownload/update/v3/static/DUProcedure/Dynamic Update.htm

For additional sources of information about performing unattended installations, see Appendix A, "Resources for learning about automated installation and deployment."

Avoiding Dynamic Update

You can avoid using Dynamic Update, which means Setup will use only the files and drivers provided on the CD for Windows XP SP1. The method by which you avoid using Dynamic Update depends on how you are performing the installation:

- **Interactive installation**: During interactive installation (not unattended installation), you can select No when offered the option to use Dynamic Update. As an alternative, you can ensure that the computer does not have Internet access.
- **Unattended Setup**: Dynamic Update is disabled when you run Setup in specific ways, as shown in the table in "How Dynamic Update communicates with sites on the Internet" earlier in this section. As the table shows, the simplest way to ensure that Dynamic Update does not run during unattended

Setup is to use the **/DUdisable** option in the command line. This ensures that Dynamic Update will not occur during the installation.

How avoiding Dynamic Update or directing Dynamic Update to a server on your network can affect users and applications

Regardless of whether you use Dynamic Update, you can obtain updated system and driver files after installations are complete (for example, through Windows Update or a service pack). Allowing Dynamic Update to run during Setup, however, helps ensure Setup success.

If you create a shared folder on a server and deliver Dynamic Update files to destination computers from that shared folder (instead of downloading the files directly from Windows Update to the computers), you can control the exact set of updated files to be installed. By contrast, when you download the current set of Dynamic Update files directly from the Windows Update Web site to users' computers, you might introduce inconsistencies among your destination computers because the Windows Web Site is periodically updated, and you cannot control when this occurs.

Procedures for controlling Dynamic Update

For detailed descriptions of Dynamic Update and procedures for controlling it, see the *Windows XP Professional Resource Kit*, specifically Chapter 2, "Automating and Customizing Installations," especially the Dynamic Update information under the overview in that chapter. To view this chapter, see the TechNet Web site at:

www.microsoft.com/technet/prodtechnol/winxppro/reskit/prbc_cai_nmip.asp

Similar information is available in the Dynamic Update article on the Microsoft Web site at:

www.download.windowsupdate.com/msdownload/update/v3/static/DUProcedure/Dynamic Update.htm

Event Viewer

The following sections provide information about:

- The benefits of Event Viewer
- How Event Viewer communicates with sites on the Internet
- How to control Event Viewer to prevent the flow of information to and from the Internet

Benefits and purposes of Event Viewer

Administrators can use Event Viewer to view and manage event logs. Event logs contain information about hardware and software problems and about security events on your computer. A computer running Microsoft Windows XP Professional Service Pack 1 (SP1) records events in three kinds of logs: application, system, and security. While Event Viewer is primarily a tool for administrators to manage event logs, users can also view application and system logs on their computer. Only administrators can gain access to security logs.

Overview: Using Event Viewer in a managed environment

Users can access event logs for their own computer through Control Panel\Administrative Tools\Event Viewer. The user can obtain detailed information about a particular event by either double-clicking the event, or selecting the event and clicking Properties on the Action menu. The dialog box gives a description of the event, which can contain one or more links to Help.

Links can either be to Microsoft servers, or to servers managed by the software vendor for the component that generated the event. On Windows XP SP1, most events that originate from Microsoft products will have standard text containing a URL at the end of the description ("For more information, see Help and Support Center at go.microsoft.com/fwlink/events.asp").

When users click the link, they are asked to confirm that the information presented to them can be sent over the Internet. If the user clicks Yes, the information listed will be sent to the Web site named in the link. The parameters in the original URL will be replaced by a standard list of parameters whose contents are detailed in the confirmation dialog box. This list is provided in the next subsection under "Specific information sent or received."

In a highly managed environment, IT administrators might want to prevent users or administrators from sending this information over the Internet through this link and accessing a Web site. In Windows XP SP1, this information flow is governed by a registry key. Administrators can edit this registry key to prevent users from accessing the Internet through Event Viewer.

How Event Viewer communicates with sites on the Internet

In order to access the relevant Help information provided by the link in the Event Properties dialog box, the user must send the information listed about the event. The collected data is confined to what is needed to retrieve more information about the event from the Microsoft Knowledge Base. User names and e-mail addresses, names of files unrelated to the logged event, computer addresses, and any other forms of personally identifiable information are not collected.

The exchange of information that takes place over the Internet is described as follows:

- **Specific information sent or received**: Information about the event sent over the Internet includes the following:
    - Company name (software vendor)
    - Date and time
    - Event ID (for example, 1704)
    - File name and version (for example, userenv.dll, 5.1.2600.1106)
    - Product name and version (for example, Microsoft Windows Operating System, 5.1.2600.1106)
    - Registry source (for example, userenv)
    - Type of event message (for example, Error)

  The information the user receives is from the Web site named in the link.
- **Default settings**: Access to Event Viewer is enabled by default.
- **Triggers**: The user chooses to send information about the event over the Internet in order to view Help.
- **User notification**: When a user clicks the link, a dialog box listing the information that will be sent is provided.
- **Logging**: This is a feature of Event Viewer.
- **Encryption**: The information may or may not be encrypted, depending on whether it is an HTTP or HTTPS link.
- **Access**: No information is stored.
- **Privacy policy**: See Event Viewer Help for a URL Privacy Policy Statement. (In Event Viewer, click **Help**, click the **Search** tab, and type "URL Privacy Policy.")
- **Port and transmission protocol**: Communication occurs over the standard port for the protocol in the URL, either HTTP or HTTPS.
- **Ability to disable**: The ability to send information over the Internet or to be linked to a Web site can be prevented by editing the registry.

Controlling Event Viewer to prevent the flow of information to and from the Internet

You can prevent users from sending information across the Internet and accessing Internet sites through Event Viewer by editing the registry. When you edit the registry as described in the following subsection, clicking Yes as previously described will still start Help, but it will not access the Internet for information specific to the event.

The Windows XP SP1 computer registry values listed in this subsection are located in the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version \Event Viewer

The following list describes how this registry key controls the flow of information to and from the Internet.

- **MicrosoftRedirectionProgram**

Default value: %SystemRoot%\PCHealth\HelpCtr\Binaries\HelpCtr.exe

Usage: This program is started with command-line parameters from MicrosoftRedirectionProgramCommandLineParameters.

- **MicrosoftRedirectionProgramCommandLineParameters**

  Default value: -url hcp://services/centers/support?topic=%s

  Usage: "%s" is replaced with the URL in the link.

- **MicrosoftRedirectionURL**

  Default value: http://go.microsoft.com/fwlink/events.asp

  Usage: Governs the text of the standard link for Microsoft events.

Note If any of these registry values is missing or empty, the link will be started directly using ShellExecute; deleting these values is not a method for preventing information from reaching the Internet.

Procedures for preventing the flow of information to and from the Internet through Event Viewer

To prevent the flow of information to and from the Internet through Event Viewer you need to edit the registry. You can then apply the registry change to computers in a domain using Group Policy.

Editing the registry

Edit HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version \Event Viewer as follows:

To prevent the user from accessing the Internet when they click the link, delete the final "%s" from the value of MicrosoftRedirectionProgramCommandLineParameters (see the previous list). With this change, clicking the link and clicking Yes will still start Help, but it will not access the Internet for information specific to this event.

For information about editing the registry, see Windows 2000 Server Help or Windows 2000 Server Resource Kit: Supplement 1 on the following Web site, and in the table of contents, navigate to Windows 2000 Registry Reference.

www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp

Caution Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on the computer. You can also use the Last Known Good Configuration startup option if you encounter problems after manual changes have been applied.

Distributing the registry change using Group Policy

You can distribute this registry change to computers in a domain by configuring a Group Policy object (GPO). You first need to create a template using the Event Viewer snap-in as described in the following procedure.

To enable the Event Viewer Group Policy snap-in

5. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.
   For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for learning about Group Policy."
6. Click **User Configuration**, click **Administrative Templates**, and then click **Windows Components**.
7. Click **Microsoft Management Console** and then click **Restricted/Permitted snap-ins**.
8. In the details pane under Setting, double-click **Event Viewer**.
9. In the Event Viewer Properties dialog box, select **Enabled**.

File association Web service

The following subsections provide information about:

- The benefits of the file association Web service
- How the file association Web service communicates with sites on the Internet
- How to control the file association Web service to limit the flow of information to and from the Internet

Benefits and purposes of the file association Web service

The file association Web service in Microsoft Windows XP Professional Service Pack 1 (SP1) extends the scope of information stored locally by the operating system about file name extensions, file types, and the applications or components to use when opening a particular file type. Both the locally stored information and the file association Web service are intended to provide the user with the ability to open (double-click) a file without having to specify which application or component to open it with. The operating system associates the file name extension (for example, .txt or .jpg) with a file type, and it opens each file type with the application or component specified for that file type. For example, file name extensions .htm and .html are both "HTML Document" file types.

The operating system first checks for the file association information locally. If no local information is available about the file name extension and its associated file type, the operating system offers the user the option of looking for more information on a Microsoft Web site. For details about the URL for this Web site, see "How the file association Web service communicates with sites on the Internet," later in this section.

Overview: Using the file association Web service in a managed environment

To limit the flow of information from the file association Web service to the Internet, you have several options. You can use firewall settings, you can disable the file association Web service by setting a registry key, you can configure automatic server-based software installation through Group Policy, and you can train users so that they understand how to specify an association between a file type and the application or component that is used to open that file type. You can also use scripts to limit the file types that users can store, view, or use, which will limit the likelihood that users will need to obtain information about those file types.

How the file association Web service communicates with sites on the Internet

The file association Web service communicates with sites on the Internet as follows:

- **Specific information sent or received**: If the operating system does not find local information about a file name extension, it offers the user the option of sending a query to look for more information on a Microsoft Web site. The site is language-specific; the file name extension that the user double-clicks is appended to the query. The query takes the following form:

  http://shell.windows.com/fileassoc/*nnnn***/xml/redir.asp?Ext=***AAA* where *nnnn* is a hexadecimal value used in Windows XP to map to a language identifier (that is, to an RFC1766 identifier), and *AAA* is the file name extension for which information is needed. An example of a hexadecimal value and its corresponding language identifier is 0409 for en-us, English (United States).

Notes
For more information about these hexadecimal values, see information about the multiple language (MLang) registry settings on the Microsoft Developer Network Web site at:
msdn.microsoft.com/library/default.asp?url=/library/en-us/wceielng/htm/cooriMLangRegistrySettings.asp

To search for information about MLang registry settings or the Microsoft Internet Explorer Multiple Language application programming interface (MLang API), use the Search tool on the Microsoft Developer Network Web site at:
msdn.microsoft.com/

- **Default setting and ability to disable**: The service is enabled by default. It can be disabled by setting a registry key, as described in "Disabling the file association Web service" later in this section.

  You can also prevent the file association Web service from being triggered by file name extensions that you know your users will occasionally encounter by configuring automatic, server-based software installation based on Group Policy settings. To learn more about this, see "Finding information about the Software Installation extension of the Group Policy snap-in" later in this section.

- **Trigger and user notification**: When the user tries to open a file (for example, by double-clicking the file), and there is no local information about the correct application or component to use when opening the file, the operating system offers the user the option either to "Use the Web service to find the appropriate program" or to "Select the program from a list."

- **Logging**: No events are logged by the file association Web service.

- **Encryption, storage, and privacy**: The file name extension sent in a query to the Internet is not encrypted. Nothing in the query identifies the user. If the local computer's browser is configured to store information about recently visited Internet sites, the browser will store the query containing the file name extension. Otherwise, the query containing the file name extension is not stored anywhere.

- **Transmission protocol and port**: The transmission protocol is HTTP and the port is 80.

Controlling the file association Web service to limit the flow of information to and from the Internet

If you want to limit the flow of information from the file association Web service to the Internet, you can use one or more of the following methods:

- Use your firewall to keep users from gaining access to any Web site that contains the following string: http://shell.windows.com/fileassoc/

- Disable the file association Web service by setting a registry key, as described in "Disabling the file association Web service" later in this section.

- Configure automatic, server-based software installation. To do this, configure your servers with the Software Installation extension of the Group Policy snap-in in Windows 2000 Service Pack 3 (SP3). When you do this, if a user tries to open a file for which the corresponding application is not installed locally, a copy of the application (stored on a server) is installed automatically. In this situation, the file association Web service will not be triggered. To learn more about the Software Installation extension, see "Finding information about the Software Installation extension of the Group Policy snap-in" later in this section.

- Train users to work with file associations as follows:
  - Instruct users that an association exists (stored by the local operating system) between a file name extension, a file type, and the application or component that is used to open that file type.
  - Provide users with information about the file name extensions for the files they need to work with most often, the file type for each extension, and the application that should be used to open each file type. For example, file name extensions .htm and .html are both "HTML Document" file types.
  - Show users how to use Control Panel, Folder Options, and the File Type tab in Folder Options to associate a file name extension with a file type, and a file type with an application. Explain to them that the operating system stores this information on the local computer.
  - Instruct users to always click "Select the program from a list" if they see a message box offering the two options, "Use the Web service to find the appropriate program" or "Select the program from a list."
- Use scripts to scan your organization’s computers for file types that you do not want users to store, view, or use. Take actions to ensure that these files do not remain on individual computers’ hard disks. If unwanted file types do not exist on the hard disks, it decreases the need for the user to obtain information about the file name extension used for that file type.

How using a firewall to block access to the file association Web site can affect users

If you use your firewall to keep users from gaining access to http://shell.windows.com/fileassoc/, users will require other sources of information in order to work with unfamiliar file types. For example, if users in the normal course of work are sent a file with an unfamiliar file name extension, and the operating system does not have locally stored information about that file name extension (or about the file type, or the application or component to use when opening the file), users will need other sources of information to work with the file, such as a document posted on your organization’s intranet.

Procedures that limit Internet communication generated by the file association Web service

This section contains the following information:

- A procedure for disabling the file association Web service by setting a registry key.
- A link to information about configuring automatic, server-based software installation through the Software Installation extension of the Group Policy snap-in in Windows 2000 SP3.
- Procedures that can be used as a basis for training users about file name extensions, file types, and the application or component that the operating system uses when opening a specific file type.

Disabling the file association Web service

The following procedure explains how to disable the file association Web service by setting a registry key.

To disable the file association Web service by setting a registry key

1. Open Registry Editor by clicking **Start**, clicking **Run**, and then typing **regedit**.

Caution Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on the computer. You can also use the Last Known Good Configuration startup option if you encounter problems after manual changes have been applied.

2. Navigate to the following registry key:

   HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System
3. Point to **New** in the **Edit** menu, and then click **DWORD Value**.
4. Type the following name:
   NoInternetOpenWith
5. Click the new entry (**NoInternetOpenWith**), and then select **Modify** in the **Edit** menu.
6. Ensure that **Hexadecimal** is selected, and then for **Value data**, type:
   1
7. Close Registry Editor.

Finding information about the Software Installation extension of the Group Policy snap-in

If you are not already familiar with using the Software Installation extension of the Group Policy snap-in on a server running Windows 2000 SP3, you can use the following procedure to learn more. For additional information about Group Policy, see the following appendices in this white paper:

- Appendix B, "Resources for learning about Group Policy."
- Appendix C, "Importing Group Policy settings for Windows XP to a server running Windows 2000 SP3."

To find information about the Software Installation extension of the Group Policy snap-in

1. On a computer running Windows 2000 SP3, click **Start**, and then click **Help**.

   As an alternative, you can view the Help for Windows 2000 products on the Web at:

   www.microsoft.com/windows2000/techinfo/proddoc/
2. On the Contents tab in Help, navigate as follows:

   Users and Computers\Group Policy\Concepts\Group Policy Overview\Software Installation

Specifying associations between file name extensions, file types, and applications or components

You can use the following procedures as a basis for training users about file name extensions, file types, and the application or component that the operating system uses when opening a specific file type.

To associate a file name extension with a file type

1. Click **Start**, and then either click **Control Panel**, or point to **Settings** and then click **Control Panel**.
2. Double-click **Folder Options**, and then click the **File Types** tab.

3. Click **New**.
4. Type a new or existing file name extension, and then click **Advanced**.
5. In **Associated File Type**:

   - Type or select **New** to create a file type to associate with the file name extension.
     -or-

   - Type or select a different file type to associate with the extension.

Note When you type a file name extension in the Create New Extension dialog box, the Associated File Type list displays the file type that is associated with that extension. To select New, scroll to the top of the list.

To associate a file name extension with an application

1. Click **Start**, and then either click **Control Panel**, or point to **Settings** and then click **Control Panel**.
2. Double-click **Folder Options**, and then click the **File Types** tab.
3. Under **Registered file types**, click a file type.
4. Click **Change**, and choose the application you want to use to open this file.

Help and Support Center: The Headlines and Online Search features

The following sections provide information about:

- The benefits of the Headlines and Online Search features in Help and Support Center
- How the Headlines and Online Search features communicate with sites on the Internet
- How to control the Headlines and Online Search features to limit the flow of information to and from the Internet

Benefits and purposes of Headlines and Online Search

Help and Support Center is a self-help portal that was first included in Microsoft Windows Millennium Edition. It is also included in all versions of Windows XP, including Windows XP Professional Service Pack 1 (SP1). Users access Help and Support Center in a number of ways, including:

- Selecting Help and Support from the Start menu.
- Selecting Help and Support from the Help menus for Control Panel, My Network Places, My Pictures, My Computer, My Music, or My Documents.

A useful feature of Help and Support Center is the Headlines area. This area is typically titled "Did you know?" and is usually located in the lower-right corner of the main window, unless the window has been customized by the OEM or modified for certain languages. A page in Help and Support Center with more Headlines is exposed to users when they click the "View more headlines" hyperlink at the bottom of the "Did you know?" section. Headlines provides a dynamic source of content that users can visit frequently to find help and support on current issues as well as those that were known at the time the operating system was released. For example, it may display links to topics that inform the user about new security bulletins, software updates, or new Help content.

Online Search, another useful feature of Help and Support Center, enables users to query online Web sites automatically when performing a search. By default, the Microsoft Knowledge Base is designated as one of the Web sites for online searches. OEMs often customize the Online Search feature by, for example, adding a check box to the search window to enable the search engine to query their OEM-specific Web sites for results. To produce the most informative results when querying the Microsoft Knowledge Base, certain information such as the version of the product installed is collected from the user’s computer and uploaded to the servers hosting the Microsoft Knowledge Base.

Overview: Using Headlines and Online Search in a managed environment

In a managed environment it is unlikely that users will be allowed unfettered access to the Internet; this would normally be controlled in some fashion by the IT department.

By creating a system registry key, or by performing unattended installation with an appropriate entry in your answer file, or using other tools available in the Windows user interface, you can control the extent to which the Headlines and Online Search features access the Internet. More details on the methods and procedures for controlling these features are described in the following subsections.

How Headlines and Online Search communicate with sites on the Internet

Headlines in Help and Support Center

The Headlines area is updated only when there is Internet connectivity. The user is not required or prompted to connect to the Internet. Help and Support Center uses information contained in the NewsSet.xml file (stored in the %windir%\pchealth\helpctr\Config folder) on the user's computer to determine:

- Whether or not to update the Headlines area
- How frequently to update the Headlines area
- Where on the Internet to obtain the Headlines updates

This subsection summarizes the communication process:

- **Specific information sent or received**: If there is Internet connectivity, when the user starts Help and Support Center, the Help and Support service (helpsvc) compares the current date to the date specified by the TIMESTAMP attribute in the NewsSet.xml file and calculates the total number of days that have elapsed since the last time Headlines was successfully updated.

  Then, if the number of elapsed days is greater than the number of days specified by the FREQUENCY attribute in NewsSet.xml, the Help and Support service connects to the Web site specified by the URL attribute and downloads an updated version of the file NewsVer.xml to the %windir%\pchealth\helpctr\Config\News folder. The user is not uniquely identified.

  Note For Headlines supplied by Microsoft, the URL attribute is:
  http://go.microsoft.com/fwlink/?LinkID=11
  For Windows XP, this currently redirects the user to the following site:
  windows.microsoft.com/windowsxp/newsver.xml

- The downloaded NewsVer.xml file contains the links to the news content files (known as news blocks) for the Windows XP operating system and the language installed on the user's computer. These news blocks contain the information used to update the Headlines area, that is, links to and descriptions of the latest information from Help and Support Center, Windows, or support-related articles posted on Microsoft Web sites, such as the Windows XP site (www.microsoft.com/windowsxp/).

  Note If the OEM has customized the Headlines feature, then the OEM-supplied Headlines may have links to the OEM's Web site.

- If there is no Internet connectivity, Help and Support Center displays an offline message similar to the following in the Headlines area:

  > When you are connected to the Internet, this area will display links to timely help and support information. If you want to connect to the Internet now, start the New Connection Wizard and see how to establish a Web connection through an Internet service provider.

- **Default and recommended settings**: The Headlines feature is enabled by default. Recommended settings are described in the next subsection, "Controlling Headlines and Online Search to limit the flow of information to and from the Internet."
- **Triggers**: The Headlines feature is automatically triggered if there is Internet connectivity when the user starts Help and Support Center.
- **User notification**: Users are not given the choice to select whether or not to update the Headlines area before an update is performed. An "Updating …" status indicator is displayed in the Headlines

area, however, to indicate when an update is being performed. Once Help and Support Center has completed checking for new headlines, the Headlines area is labeled "Updated: *date*," where *date* is the current date.

- **Logging**: There is no information related to Headlines entered into the event log.
- **Encryption**: The data transferred to Microsoft is not encrypted.
- **Access**: The Microsoft product group has access to the raw data only.
- **Transmission protocol and port**: The transmission protocol used is HTTP and the port is 80.
- **Ability to disable**: You can disable Headlines by setting a registry key or during unattended installations. For more information, see "Procedures for disabling Headlines and Online Search" later in this section.

Online Search in Help and Support Center

Online Search can only query online Web sites like the Microsoft Knowledge Base when there is Internet connectivity; users are neither required nor prompted to connect to the Internet. When users perform a search in Help and Support Center, the search engine automatically checks the online Microsoft Knowledge Base and other OEM-designated Web sites for results to their search query.

This subsection summarizes the communication process:

- **Specific information sent or received**: To produce relevant results when querying the Microsoft Knowledge Base, certain information is collected from the user’s computer and uploaded to a server at Microsoft that hosts the Microsoft Knowledge Base. The user is not uniquely identified. Following is a list of the information collected:
  - The search text string entered by the user
  - The language code of the operating system
  - The product Knowledge Base to be searched (for example, Windows XP or Outlook)
  - The SKU of the operating system installed (for example, Home Edition, Professional, or Server)
  - The number of results the user has indicated that they want in their result set
  - Titles field status (indicates whether or not to search the article title only)
  - Type field status (indicates whether to search using "all" or "any" of the search string)
- **Default and recommended settings**: Online Search is enabled by default. Recommended settings are described in the next subsection, "Controlling Headlines and Online Search to limit the flow of information to and from the Internet."
- **Triggers**: Online Search is automatically triggered if there is Internet connectivity when the user performs a search using Help and Support Center.
- **User notification**: Users are not notified when Help and Support Center performs an Online Search. A permanent headline is provided in the Headlines area that instructs users about setting their Online Search options, including how to turn the feature off.
- **Logging**: There is no information related to Online Search entered into the event log.
- **Encryption**: The data transferred to Microsoft is not encrypted.
- **Access**: The data uploaded to the server is aggregated and clustered. Information about the most common queries is later made available to the Windows Product Support Services and Windows User Assistance teams to help in developing new content or in revising existing content.

- **Privacy policy**: Microsoft does not retrieve any personally identifiable information from a user's computer during an online search. A permanent headline is provided in the Headlines area that instructs users about setting their Online Search options, including how to turn the feature off.
- **Transmission protocol and port**: The transmission protocol used is HTTP and the port is 80.
- **Ability to disable**: You can disable Online Search through the Help and Support Center user interface.

Controlling Headlines and Online Search to limit the flow of information to and from the Internet

Using the appropriate system registry key, or performing unattended installation with an appropriate entry in your answer file, you can disable the Headlines feature and eliminate the entire "Did you know?" area in the Help and Support Center user interface. If you perform unattended installation, the answer file entry is as follows:

```
[PCHealth]
Headlines = 0
```

You can also configure the user interface to disable the Online Search feature. For more information, see "Procedures for disabling Headlines and Online Search" later in this section.

Configuration settings for Headlines and Online Search

Headlines: Configuration tool	**Setting**	**Result**
Unattended Installation	Include Headlines = 0 under the [PCHealth] section.	Replaces text in Headlines area with white space.
Registry	Set HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ PCHealth\HelpSvc\Headlines equal to 0.	Replaces text in Headlines area with white space.
Search: Configuration tool	**Setting**	**Result**
Help and Support Center user interface (Set Search Options window)	Clear any check boxes for querying the Microsoft Knowledge Base or OEM Web sites for results.	Disables online searches. The search results window neither displays an area for the online Web sites (such as the Microsoft Knowledge Base) nor returns any search results from online Web sites.
Headlines and Search: Configuration tool	**Setting**	**Result**
Firewall	Block HTTP port 80.	Displays offline message text in Headlines area. The search results window displays an area for the online Web sites (such as the Microsoft Knowledge Base), but does not return any search results from online Web sites.

How controlling Headlines and Online Search can affect users and applications

The Headlines area provides a good way for users to obtain up-to-date solutions to common problems, updated self-help content, and information about software and driver updates. If you decide to disable the Headlines feature, the Headlines ("Did you know?") area in the Help and Support Center user interface will be blank and links to new content or software update notifications will never be presented to the user.

The Online Search feature enables users to obtain help from online Web sites and can often reduce the support load on the internal Help desk. If you decide to disable the Online Search feature, users will only be able to query local Help content.

Disabling Headlines and Online Search will not affect any other applications.

Alternate methods for controlling Headlines and Online Search

You can configure your firewall to restrict access to the Internet through HTTP port 80. You can also use the firewall to block updates to the Headlines area and to block online searches. In this scenario, for the Headlines feature, Help and Support Center displays the offline message text described in "How Headlines and Online Search communicate with sites on the Internet." When traffic through HTTP port 80 is blocked in this way, Help and Support Center searches will only query local Help content. The search results window will display an area for the online Web sites, such as the Microsoft Knowledge Base, but it will not contain any results.

For more information about firewalls, see Appendix E, "Internet Connection Sharing and Internet Connection Firewall."

Procedures for disabling Headlines and Online Search

You can disable the Headlines feature on individual computers running Windows XP by modifying the system registry.

To disable the Headlines feature on individual computers

1. Open Registry Editor.
2. In the registry tree (on the left), navigate to the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PCHealth\HelpSvc\.
3. On the **Edit** menu, point to **New**, and then click **DWORD value**.
4. Type **Headlines** as the name for the new value (type REG_DWORD), and then press ENTER.

   Note Setting the data value to 0 (or leaving the default for a new REG_DWORD) disables Headlines. If the Headlines REG_DWORD has another value or doesn't exist, then Headlines is enabled.

You can disable the Headlines feature during workstation deployment by using standard methods for unattended installation or remote installation.

To disable the Headlines feature during unattended installation by using an answer file

1. Using the methods you prefer for unattended installation or remote installation, create an answer file. For more information about unattended and remote installation, see Appendix A, "Resources for learning about automated installation and deployment."
2. In the [PCHealth] section of the answer file, include the following entry:

   Headlines = 0

   Note Headlines = 0 specifies that no information is displayed in the Headlines ("Did you know?") area on the Help and Support Center home page. Headlines = 1 specifies that Headlines is displayed.

Formatted: Bullets and Numbering

You can turn off online searches in the Help and Support Center user interface.

To disable the Online Search feature on individual computers

1. Click **Start**, and then click **Help and Support**.
2. Below the Search box, click **Set search options**.
3. Click to clear the **Microsoft Knowledge Base** check box and any other check boxes below it. For example, the manufacturer of your computer may have added a check box to allow your search to query their Web site for results.
4. Close Help and Support Center.

Internet Explorer 6 SP1

This section provides information about:

- The benefits of Microsoft Internet Explorer 6 Service Pack 1 (SP1) in Windows XP Professional Service Pack 1 (SP1).
- Steps for planning and deploying configurations for Internet Explorer 6 SP1 in a way that balances your users' requirements for Internet access with your organization's requirements for protection of networked assets.

  If you decide that you do not want users to have access to Internet Explorer, see "Excluding Internet Explorer 6 SP1 from the desktop," later in this section.
- Examples of the security-related features offered in Internet Explorer 6 SP1 (as compared to Internet Explorer 5).
- Resources for learning about topics related to security in Internet Explorer 6 SP1. This includes resources that help you learn about:
  - Security and privacy settings in Internet Explorer 6 SP1.
  - Mitigating the risks inherent in Web-based applications and scripts.
  - Methods for deploying specific configurations of Internet Explorer 6 SP1 across your organization using Group Policy, the Internet Explorer Administration Kit (IEAK), or both.

Notes
This section of the white paper describes Internet Explorer 6 SP1 in general, but it does not describe Outlook Express 6 (the e-mail component in Internet Explorer 6 SP1), the New Connection Wizard, or the error reporting tool in Internet Explorer. For information about these components, see the respective sections of this white paper (the error reporting tool in Internet Explorer is described in the "Windows Error Reporting" section of this white paper).

Also note that the New Connection Wizard replaces the Network Connection Wizard and the Internet Connection Wizard in Windows 2000.

It is beyond the scope of this white paper to describe all aspects of maintaining appropriate levels of security in an organization where users connect to Web sites, run software from the Internet, download items from the Internet, and perform similar actions. This section, however, provides overview information as well as suggestions for other sources of information about how to balance users' requirements for Internet access with your organization's requirements for protection of networked assets.

For more information about Internet Explorer, see the following resources:

- Help for Internet Explorer (with Internet Explorer open, click the Help menu and select an appropriate option)
- The Internet Explorer page on the Microsoft Web site at:

  www.microsoft.com/windows/ie/
- The Resource Kit for Internet Explorer. To learn about this and other Resource Kits, see the Windows Deployment and Resource Kits Web site at:

  www.microsoft.com/reskit/

Benefits and purposes of Internet Explorer 6 SP1

Internet Explorer 6 SP1 is designed to make it easy to browse and interact with sites on an intranet or on the Internet. It differs from most of the other components described in this white paper in that its main function is to communicate with sites on the Internet or an intranet (which contrasts with components that communicate with the Internet in the process of supporting some other activity).

Internet Explorer 6 SP1 is also designed to be highly configurable by an administrator (or in an unmanaged environment, a user), with security and privacy settings that can protect your organization’s networked assets while at the same time providing users with access to useful information and tools.

Internet Explorer 6 SP1 offers more security-related options and settings than were available in Internet Explorer 5. With an understanding of the settings and options available in Internet Explorer 6 SP1, you can choose the settings appropriate to your organization’s requirements, and create a plan for one or more standard Internet Explorer configurations. After planning your standard configurations, you can use deployment tools to deploy and maintain them. The subsections that follow provide more information about these steps.

Steps for planning and deploying configurations for Internet Explorer 6 SP1

This section outlines a list of steps that can help you deploy Internet Explorer 6 SP1 in a way that provides users with Internet access, while at the same time providing your organization’s networked assets with an appropriate level of protection from the risks inherent in the Internet. (If you prefer to remove all visible entry points to Internet Explorer when you perform unattended installation, see "Excluding Internet Explorer 6 SP1 from the desktop," later in this subsection.)

A recommended set of steps is:

- Assess the other elements in your security plan that will work together with Internet Explorer 6 SP1 to provide users with access to the Internet while still providing an appropriate degree of protection for your organization’s networked assets. These elements include:

  - Your proxy server.
  - Your firewall.
  - Your basic security measures, as described in the introduction to this white paper. These security measures include using virus-protection software and setting requirements for strong passwords.

  It is beyond the scope of this white paper to provide detailed recommendations for these security elements. For more information about security, see the references listed in the introduction, as well as the documentation for your proxy server, firewall, virus-protection software, and other software you use to protect networked assets.

- Learn about the security-related features offered in Internet Explorer 6 SP1, some of which are described in "Examples of the security-related features offered in Internet Explorer 6 SP1," later in this section. Using information about these features, identify the ones of most value for your business and security requirements.

- Learn how to configure security settings in Internet Explorer 6 SP1, as described in "Learning about security and privacy settings in Internet Explorer 6 SP1," later in this section.

- Learn about ways to mitigate the risks inherent in code that can be run through a browser, as described in "Learning about mitigating the risks inherent in Web-based programs and scripts," later in this section.

- After gathering information about the previous three items (security-related features, security settings, risks inherent in code), plan one or more standard Internet Explorer configurations for the desktops in your organization.
- Learn about ways of deploying configurations of Internet Explorer 6 SP1 across your organization:
  - Learn about using Group Policy to control the configuration of Internet Explorer 6 SP1 on desktops across your organization, as described in "Learning about Group Policy objects that control configuration settings for Internet Explorer 6 SP1," later in this section.
  - Learn about the deployment technologies available in the Internet Explorer Administration Kit (IEAK) 6 SP1, some of which are described in "Learning about the Internet Explorer Administration Kit," later in this section.

  Using the information about Group Policy and the IEAK, create a plan for deploying and maintaining your standard Internet Explorer configurations.

Excluding Internet Explorer 6 SP1 from the desktop

As an alternative to the use of Internet Explorer 6 SP1 in your organization, you can remove all visible entry points to Internet Explorer. You can do this during workstation deployment by using standard methods for unattended installation or remote installation. If you are using an answer file, the entry is as follows:

```
[Components]
IEAccess = Off
```

For complete details about how the IEAccess entry works, see the resources listed in Appendix A, "Resources for learning about automated installation and deployment." Be sure to review the information in the Deploy.chm file (whose location is provided in that appendix).

Examples of the security-related features offered in Internet Explorer 6 SP1

This subsection describes enhancements in some of the security-related features in Internet Explorer 6 SP1, as compared to Internet Explorer 5. These features include:

- A Privacy tab that provides greater flexibility in specifying whether cookies will be blocked from specific sites or types of sites. An example of a type of site that could be blocked is one that does not have a compact policy, that is, a condensed computer-readable privacy statement. (The Privacy tab was not available in Internet Explorer 5.)
- Security settings that specify how Internet Explorer 6 SP1 handles such higher-risk items as ActiveX controls, downloads, and scripts. These settings can be customized as needed, or they can be set to these predefined levels: high, medium, medium-low, or low. You can specify different settings for a number of zones, the most basic being the four preconfigured zones:
  - Local intranet zone: Contains addresses inside your proxy server.
  - Trusted sites: Includes sites you designate as "trusted."
  - Restricted sites: Includes sites you designate as "restricted."
  - Internet zone: Includes everything that is not in another zone and is not on the local computer.

  You can also specify different settings for the following zones:

  - My computer zone: This is a zone configurable only through the IEAK. It contains files on the local computer. Configuration settings for this zone are not available in the browser interface.
  - Customized zones: These are added programmatically using the URL security zones application programming interface (API). For more information about this API, see the Microsoft Developer Network Web site at:

    msdn.microsoft.com/

- Support for content-restricted IFrames (inline floating frames). This type of support enables developers to implement these frames in a way that makes it more difficult for malicious authors to start e-mail or content-based attacks.
- Improvements to Service Pack 1 that increase the overall security and reliability of Internet Explorer 6.

For more information about features available in Internet Explorer, see the information in the next subsection, as well as the Internet Explorer page on the Microsoft Web site at:

www.microsoft.com/windows/ie/

Resources for learning about topics related to security in Internet Explorer 6 SP1

This subsection lists resources that can help you learn about the following topics related to security in Internet Explorer 6 SP1:

- Security and privacy settings available in Internet Explorer 6 SP1
- Methods for mitigating the risks inherent in Web-based programs and scripts
- Ways to use Group Policy objects that control configuration settings for Internet Explorer 6 SP1
- The Internet Explorer Administration Kit

In addition, for information about unattended installation, see the resources listed in Appendix A, "Resources for learning about automated installation and deployment."

Learning about security and privacy settings in Internet Explorer 6 SP1

An important source of detailed information about security and privacy settings in Internet Explorer 6 SP1 is the Microsoft Internet Explorer 6 Resource Kit. To learn about this and other resource kits, see the Windows Deployment and Resource Kits Web site at:

www.microsoft.com/reskit/

The Microsoft Internet Explorer 6 Resource Kit consists of a number of parts that include these titles:

- "Privacy and Security Features"
- "Preparation for Deployment"
- "Customization and Installation"
- "Maintenance and Support," including information about keeping programs updated
- Appendices, including an appendix titled "Setting System Policies and Restrictions"

Learning about mitigating the risks inherent in Web-based programs and scripts

In a network-based and Internet-based environment, programs can take a variety of forms including scripts within documents, scripts within e-mail, or programs or other code objects running within Web pages. These programs can move across the Internet and are sometimes referred to as "mobile code." Configuration settings provide ways for you to control the way Internet Explorer 6 SP1 responds when a user tries to run a particular code object. Two examples of the ways you can customize the Internet Explorer configuration deployed in your organization are as follows:

- You can control the code (ActiveX controls, scripts, and so on) that users can run. You can do this by customizing Authenticode settings, which can, for example, prevent users from running any unsigned code or enable them to only run code signed by specific authors.
- If you want to permit the use of ActiveX controls, but do not want users to download code directly from the Internet, you can specify that when Internet Explorer 6 SP1 looks for a requested executable, it goes to your own internal Web site instead of the Internet. For more information, see the white paper titled "Managing Mobile Code with Microsoft Technologies" at the end of this list, and search for CodeBaseSearchPath.

You can use the following sources to learn more about mitigating the risks inherent in Web-based programs and scripts:

- To understand more about how a particular Microsoft programming or scripting language works, see the Microsoft Developer Network Web site at:

  msdn.microsoft.com/

- To learn about approaches to mitigating the risks presented by mobile code, see "Managing Mobile Code with Microsoft Technologies," a white paper on the Technet Web site at:

  www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bestprac/mblcode.asp

Learning about Group Policy objects that control configuration settings for Internet Explorer 6 SP1

You can control configuration settings for Internet Explorer 6 SP1 by using Group Policy objects (GPOs) on servers running Windows 2000. (You can also control the configuration of Internet Explorer by using the Internet Explorer Administration Kit; for more information, see "Learning about the Internet Explorer Administration Kit," later in this section.) For sources of information about Group Policy, see the appropriate appendices in this white paper.

To learn about specific Group Policy settings that can be applied to computers running Windows XP Professional SP1, see the spreadsheet in "Windows XP Professional Resource Kit, Group Policy Object Settings" at:

www.microsoft.com/WindowsXP/pro/techinfo/productdoc/gpss.asp

Learning about the Internet Explorer Administration Kit

With the deployment technologies available in the Internet Explorer Administration Kit (IEAK), you can efficiently deploy Internet Explorer and control the configuration of Internet Explorer across your organization. (You can also control the configuration of Internet Explorer by using Group Policy; for more information, see "Learning about Group Policy objects that control configuration settings for Internet Explorer 6 SP1," earlier in this section.)

A few of the features and resources in the IEAK include:

- **Internet Explorer Customization Wizard**. Step-by-step screens guide you through the process of creating customized browser packages that can be installed on client desktops.
- **IEAK Profile Manager**. After you deploy Internet Explorer, you can use the IEAK Profile Manager to change browser settings and restrictions automatically.
- **IEAK Toolkit**. The IEAK Toolkit contains a variety of helpful tools, programs, and sample files.
- **IEAK Help**. IEAK Help includes many conceptual and procedural topics that you can view by using the Index, Contents, and Search tabs. You can also print topics from IEAK Help.

For more information about the IEAK, see the IEAK Web site at:

www.microsoft.com/windows/ieak/

Internet games on Windows XP

The following sections provide information about:

- The benefits of Internet games on Windows XP
- How Internet games on Windows XP communicate with sites on the Internet, including MSN Gaming Zone
- How to control Internet games on Windows XP to prevent the flow of information to and from the Internet

Benefits and purposes of Internet games on Windows XP

Microsoft Windows XP Professional Service Pack 1 (SP1) includes six standard games for Windows and five new Internet games as part of the installation package. These games can be accessed through the Start\All Programs\Games menu. The six standard games do not interact with the Internet in any way. The new Internet games, however, open a limited connection to the free games section of the MSN Gaming Zone, which is located at www.zone.msn.com.

The MSN Gaming Zone is part of The Microsoft Network (MSN) family of Web sites. It provides a place for users to download games, compete in interactive online gaming, and play a number of single-player games that require no interaction with other users. The MSN Gaming Zone also offers forums where individuals can chat and find other players who are interested in playing computer games.

Overview: Using Internet games on Windows XP in a managed environment

The Internet games offered in Windows XP are somewhat different from those available on the MSN Gaming Zone Web site. The versions on the MSN Gaming Zone support full chatting, the ability to customize the user's name, access to ratings and recorded scores, competitions, tournaments, and lists of contacts, among other features. The Internet games that come with Windows XP do not have any Web component in and of themselves and their functionality and communication with the gaming zone server is limited, as described in the following subsection.

The games that come packaged with Windows XP can be removed from the installation setup. By eliminating access to the Internet games on the client you will eliminate communication with MSN Gaming Zone. Direct access to this site can also be blocked at the firewall or gateway server as determined by standard IT practices within your organization.

How Internet games on Windows XP communicate with sites on the Internet

When the user navigates to Start\All Programs\Games, and then clicks one of the five Internet games listed, a dialog box opens announcing the intended connection to the free games section of the MSN Gaming Zone. (The MSN Gaming Zone is located at www.zone.msn.com; at www.zone.msn.com/hub_flog.aspyou can access the free games section directly.) The dialog box displays a warning message concerning information being passed and gives the user the option to cancel the interaction. If the user chooses to connect, a limited interactive session with other online users is established.

As mentioned previously, the free games section is part of the MSN Gaming Zone, which is an external Web site that can also be accessed directly through an Internet browser. Once connected, users can anonymously play free games or they can sign in to their account to chat, play interactive games with other users, or download new games.

This section describes various aspects of the data that is sent to and from the Internet, and how the exchange of information takes place:

- **Specific information sent or received**: MSN Web sites require a valid passport. The only additional information requested over and above a passport is a unique screen name, which is anonymous. There is no reverse lookup for this screen name and it is used to identify the user in all MSN services (rather than using the passport name, or any part of the passport identity).

  MSN uses .NET Passport to provide registration and sign-in services. MSN uses cookies and may also use Web beacons. (The Web beacon tool is not used to collect personal information; it collects only a cookie number, time and date of a page view, and a description of the page on which the Web beacon resides.)
- **Default settings**: There is no default access. A user must accept before being allowed access to the games.
- **Triggers**: Users select one of the Internet games from the Games menu.
- **User notification**: No information is sent if the user does not proceed past the splash screen. Once in the game, basic move data is passed from the client to the server.
- **Encryption**: There is no encryption of data. The chat components in the game are not free-form. Communication is limited to sending 30 pre-canned messages.
- **Access**: Games server support staff and MSN Gaming Zone operational support staff have access to the data.
- **Privacy policy**: The privacy statement associated with the MSN Gaming Zone belongs to MSN.
- **Port**: The port ranges are 28000 through 29000.
- **Transmission protocol**: The client connects to the server using a TCP/IP Winsock (Windows sockets API).
- **Ability to disable**: User acceptance is required to play the games. It is possible to uninstall the games by using Windows XP Setup, or to block access to the MSN Gaming Zone through the use of a firewall rule.
- **Uniquely identify user**: A randomly generated, globally unique identifier (GUID) is created on first use and is stored on the server. This is used to anonymously (but uniquely) identify each client connecting.

Controlling Internet games on Windows XP to prevent the flow of information to and from the Internet

The most direct method of preventing the flow of information is to remove the Internet games from the Games package of the Windows XP installation file. Since Windows XP clients connect to the games servers through a Domain Name System (DNS) entry, however, using a firewall to block the DNS entry for the MSN Gaming Zone at www.zone.msn.com will block the connection from the Windows XP game clients to the server.

To eliminate access to the MSN Gaming Zone, you can block access to the Internet or directly block access to the MSN Gaming Zone. Internet Web sites can be blocked through a proxy server, firewall, or the Microsoft Internet Security and Acceleration (ISA) Server. An administrator has the ability to specify a list of prohibited IP addresses. If a client requests access to one of these sites an error message will be returned. Procedures for removing the Internet games from installation through the GUI and by using an answer file (during unattended installation) are described in the next subsection.

Procedures for Configuration of Internet games on Windows XP

Access to the Internet games on Windows XP can be configured in several ways as described previously. This subsection describes the procedures to remove the Internet games in accordance with your company's security policies.

The following procedures provide information about:

- Removing Internet games from Windows XP installation through the GUI.
- Excluding Internet games during unattended installation of Windows XP by using an answer file.

To remove games from Windows XP installation through the GUI

1. Click **Start**, click **Settings**, click **Control Panel**, and then click **Add or Remove Programs**. (To complete this process the user must have administrative credentials.)
2. From the **Add or Remove Programs** dialog box, click **Add or Remove Windows Components**.
3. From the Windows Component Wizard, select **Accessories and Utilities**, and then click **Details**.
4. From the **Accessories and Utilities** dialog box, select **Games**, and then click **Details**.
5. From the **Games** dialog box, clear the check boxes for the games that you want to remove from the installation.
6. Click **OK**.
7. Click **OK**.
8. Click **Next** to initiate the setup. To complete the setup, the computer must have access to the original installation media, or network installation share point.

To exclude the Internet games components during unattended installation by using an answer file

1. Using the methods you prefer for unattended installation or remote installation, create an answer file. For more information about unattended and remote installation, see Appendix A, "Resources for learning about automated installation and deployment."
2. In the [Components] section of the answer file, include the following entry:

   Zonegames = Off

   Note You can also check a registry key (manually or with a script) on a computer running Windows XP SP1 to see whether the games component is installed. Do not, however, change this registry key. A registry key value of 0x00000000 means the component is not installed, and a value of 0x00000001 means the component is installed. The key is as follows:

   HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\OC Manager\Subcomponents\zonegames

Internet Information Services in Windows XP SP1

The following subsections provide information about:

- The benefits of Internet Information Services (IIS) in Microsoft Windows XP Professional Service Pack 1 (SP1).
- How to control IIS on users' computers to prevent the flow of information to and from the Internet

Benefits and purposes of IIS in Windows XP SP1

IIS 5.1 is one of the optional components in Windows XP SP1. Allowing selected users to install this component provides them with an easy way to publish information on the Internet or an intranet. IIS includes innovative security features and a broad range of administrative features for managing Web sites. By using programmatic features like Active Server Pages (ASP), users who have been given the responsibility to create Web sites can more easily create and deploy scalable, flexible Web applications.

IIS is not installed by default with Windows XP SP1 but can be added using Add or Remove Programs in Control Panel. IIS in Windows XP Professional SP1 can, by default, service only 10 simultaneous client connections, with one Web site only, and does not use all the features of the server versions. IIS 5.1 in Windows XP Professional SP1 includes the Microsoft Management Console (MMC) snap-in for managing IIS. For more information about IIS features, see the following Web sites:

- The IIS 5.1 page (part of the Windows XP Professional evaluation pages) at:

  www.microsoft.com/WindowsXP/pro/evaluation/overviews/iis.asp
- The IIS Security page (part of Technet) at:

  www.microsoft.com/technet/security/prodtech/windows/iis/default.asp

Overview: IIS on computers running Windows XP SP1 in a managed environment

In a managed environment, it is recommended that you carefully select and train any users who will be permitted to install IIS on their computers running Windows XP SP1. In some respects, such users have responsibilities like those of a server administrator, and they should therefore be trained about security, auditing, and monitoring.

It is beyond the scope of this white paper to provide details about maintaining security on a computer that hosts a Web site. Because administrators will most likely exclude IIS from standard desktop configurations in a managed environment, the sections that follow provide details about how to prevent the installation of this component.

Controlling IIS on users' computers to prevent the flow of information to and from the Internet

To maximize the security of computers in your organization and prevent the flow of information through IIS on clients running Windows XP SP1, remove or exclude this component from installation on those clients. You can do this during workstation deployment by using standard methods for unattended installation or remote installation. If you are using an answer file, the following table shows the entries, all of which are in the [Components] section.

> **Note** By default, the components listed in the table are not installed with Windows XP Professional.

The following table shows the answer file entries as well as the associated registry keys. Do not change the registry keys. They are shown for use in a script that could check whether a particular component is installed on a particular computer. A registry key value of 0x00000000 means the component is not installed, and a value of 0x00000001 means the component is installed.

Answer file entries and registry keys associated with IIS subcomponents

IIS subcomponent	**Answer file entry (in the [Components] section)**	**Registry key (for use in a script that checks whether a component is installed): 0x00000000 means it is not installed; 0x00000001 mean it is installed**
IIS common files	iis_common = Off	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\OC Manager\Subcomponents\iis_common
IIS documentation	IIS_doc = Off	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\OC Manager\Subcomponents\iis_doc
File Transfer Protocol (FTP) service	iis_ftp = Off	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\OC Manager\Subcomponents\iis_ftp
IIS MMC snap-in	iis_inetmgr = Off	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\OC Manager\Subcomponents\iis_inetmgr
Simple Mail Transfer Protocol (SMTP) service	iis_smtp = Off	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\OC Manager\Subcomponents\iis_smtp
World Wide Web (WWW) service	iis_www = Off	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\OC Manager\Subcomponents\iis_www
Not a subcomponent: specifies whether to create the optional scripts directory on the default Web site	iis_www_vdir_scripts = Off	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\OC Manager\Subcomponents\iis_www_vdir_scripts
FrontPage server extensions	fp_extensions = Off	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\OC Manager\Subcomponents\fp_extensions

Procedures for checking or preventing the installation of IIS subcomponents on a client

The following procedures explain how to:

- View the registry keys listed in the table in the previous section
- View the components currently installed on a computer running Windows XP

- Prevent the installation of IIS subcomponents during unattended installation by using an answer file

To view registry keys related to IIS subcomponents

1. Open Registry Editor by clicking **Start**, clicking **Run**, and then typing **regedit**.

   Caution Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on the computer. You can also use the Last Known Good Configuration startup option if you encounter problems after manual changes have been applied.

1. Navigate to HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\OC Manager\Subcomponents\.
2. View the registry keys listed in the table in the previous section, and the value associated with each key. A value of 0x00000000 means the component is not installed. A value of 0x00000001 means the component is installed.
3. Close Registry Editor.

To view the components currently installed on a computer running Windows XP

1. Click **Start**, and then either click **Control Panel**, or point to **Settings** and then click **Control Panel**.
2. Double-click **Add or Remove Programs**.
3. Click **Add\Remove Windows Components** (on the left).
4. Scroll down to Internet Information Services (IIS) and click **Details**.
5. View the list of subcomponents and each check box, which show whether a particular subcomponent has been installed.

To prevent the installation of IIS subcomponents during unattended installation by using an answer file

1. Using the methods you prefer for unattended installation or remote installation, create an answer file. For more information about unattended and remote installation, see Appendix A, "Resources for learning about automated installation and deployment."
2. In the [Components] section of the answer file, ensure that there are no entries for the subcomponents listed in the preceding table, "Answer file entries and registry keys associated with IIS subcomponents." If you want to list any of these subcomponents, ensure that the entries specify **Off**.

   If IIS subcomponents are not listed in an answer file for unattended installation of Windows XP Professional, by default, these subcomponents are not installed.

Internet Printing

The following sections provide information about:

- The benefits of Internet printing
- How Internet printing communicates with sites on the Internet
- How to control Internet printing to prevent the flow of information to and from the Internet

Benefits and purposes of Internet printing

Internet printing makes it possible for client computers running Microsoft Windows XP Professional Service Pack 1 (SP1) to use printers located anywhere in the world by sending print jobs using Hypertext Transfer Protocol (HTTP).

Additionally, computers running Windows XP can use Microsoft Internet Information Services (IIS) or a Web peer server to create a Web page that provides information about printers and provides the transport for printing over the Internet.

Overview: Using Internet printing in a managed environment

You need to consider both the server and client components of Internet printing:

- Server: It is possible for a user on a computer running Windows XP to install IIS and then configure that computer to act as a print server, allowing Internet printing. In a managed environment, you may want to prevent users from installing IIS, disable the Internet printing functionality of IIS, or properly secure IIS and Internet printing so that they are available only to authorized users.
- Client: Client computers can install an Internet printer using a Web browser, the Add Printer Wizard, or the Run dialog box. In order to prevent Internet printing, you must remove the ability for users to add an Internet printer.

Details on how to configure your Windows XP implementation to achieve these goals can be found later in this section.

How Internet printing communicates with sites on the Internet

The Internet printing process is as follows:

1. A user connects to a print server over the Internet by typing the URL for the print device.
2. The HTTP request is sent over the Internet to the print server.
3. The print server requires the client to provide authentication information. This ensures that only authorized users print documents on the print server.
4. After a user has authorized access to the print server, the server presents status information to the user by using Active Server Pages (ASP), which contain information about currently available printers.
5. When the user connects to any of the printers on the Internet printing Web page, the Windows XP client first tries to find a driver for the printer locally. If an appropriate driver cannot be found, the print server generates a cabinet file (.cab file, also known as a setup file) that contains the appropriate

printer driver files. The print server downloads the .cab file to the client computer. The user on the client computer is prompted for permission to download the .cab file.

6. After users connect to an Internet printer, they can send documents to the print server by using Internet Printing Protocol (IPP).

Communication for Internet printing uses IPP and HTTP (or HTTPS) over any port that the print server has configured for this service. Because the service is using HTTP or HTTPS, this is typically port 80 or 443. Because Internet printing does support HTTPS traffic, communication can be encrypted, depending on the user’s Internet browser settings.

Client computers running Windows XP can use Internet printing by default. Users must be authenticated by the print server, however, before they can use any of the printers connected to that server. If you install IIS on Windows XP, Internet printing is automatically enabled as a feature of IIS. As described earlier, you can disable or restrict computers running Windows XP from hosting Internet printing through a variety of methods. See the following subsections for additional details.

The print server can use IIS and other technologies to collect and log extensive data about the user, the computer that sends the printing request, and the request itself. It is beyond the scope of this white paper to describe Web site operations and the specifics of what type of information can be collected. For more information about IIS and other related resources, see "Internet Information Services in Windows XP SP1" in this white paper.

Controlling Internet printing to prevent the flow of information to and from the Internet

Client computers

To prevent the use of Internet printing from a client computer running Windows XP, you can delete the registry key that the Print Spooler service uses to load the Internet print provider. The procedure for this method is provided in the next subsection.

How deleting the Internet print provider registry key can affect users and applications

Deleting the Internet print provider registry key on a client computer will prevent users of that computer from using Internet printing through the Run dialog box, the Add Printer Wizard, and the browser. Deleting this key, however, may affect other print operations.

Print servers

As described earlier, users on a computer running Windows XP can install IIS and can then configure that computer to act as a print server, allowing Internet printing from other computers. In order to control this, you can use Group Policy to:

- Prevent users from installing IIS (recommended)
- Disable Internet printing when IIS is installed
- Restrict access to the printer to limited user IDs

Procedures for disabling Internet printing

Procedures for disabling Internet printing on a client computer running Windows XP

To prevent users from using Internet printing on a client computer running Windows XP, delete the Internet print provider registry key as described in the following procedure. This procedure must be performed on every computer running Windows XP in your organization. In order to ensure that these actions are correctly performed on all computers, consider using an automated setup routine or script.

To delete the Internet print provider registry key

1. Click **Start**, and then either click **Control Panel**, or point to **Settings** and then click **Control Panel**.
2. Double-click **Administrative Tools**, and then double-click **Services**.
3. Stop the Print Spooler service.
4. Use the Microsoft Registry Editor (regedit.exe) to delete the following key from the registry:
5. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Providers\Internet Print Provider
6. Restart the Print Spooler service.

Caution Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on the computer. You can also use the Last Known Good Configuration startup option if you encounter problems after manual changes have been applied.

Procedures for disabling Internet printing on a computer running IIS

It is recommended that you prevent users from installing IIS. More details on how to achieve this can be found in "Internet Information Services in Windows XP SP1" in this white paper.

The next best option is to disable Internet printing on the computer that is running IIS. The following procedure describes how to do this through Group Policy.

To disable Internet printing using Group Policy

1. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.
   For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for learning about Group Policy."
2. Click **Computer Configuration**, click **Administrative Templates**, and then click **Printers**.
3. In the details pane, double-click **Web-based Printing**.
4. Select **Disabled**.

Note This Group Policy setting is equivalent to setting the registry entry \\Hkey_Local_Machine\Software\Policies\Microsoft\Windows NT\Printers to DisableWebPrinters.

Related Links

For more information on managing Windows XP in a Windows 2000 Server environment, see the white paper at:

www.microsoft.com/windowsxp/pro/techinfo/administration/policy/default.asp

For general information on Group Policy, see Appendix B, "Resources for learning about Group Policy" and Appendix C, "Importing Group Policy settings for Windows XP to a server running Windows 2000 SP3."

To learn about specific Group Policy settings that can be applied to computers running Windows XP Professional SP1, see the spreadsheet titled "Windows XP Professional Resource Kit, Group Policy Object Settings" at:

www.microsoft.com/WindowsXP/pro/techinfo/productdoc/gpss.asp

For more information on the use of IIS in a controlled environment, see "Internet Information Services in Windows XP SP1" in this white paper.

For more information about Internet printing, see the article "Overview of Internet Printing in Windows 2000" in the Microsoft Knowledge Base. You can search the Knowledge Base by going to:

support.microsoft.com/

and then following the instructions on the page. Search for "Internet printing."

Internet Protocol version 6 (IPv6)

The following sections provide information about:

- An introduction to the IPv6 protocol
- The benefits of the IPv6 protocol
- How the IPv6 protocol communicates with sites on the Internet
- How to control the IPv6 protocol to limit the flow of information to and from the Internet
- How to monitor and troubleshoot the IPv6 protocol after configuration is complete

An introduction to the IPv6 protocol

The current version of the Internet Protocol (known as IP version 4 or IPv4) has not been substantially changed since 1981, when the Internet Engineering Task Force (IETF) published the definitive specification of IP (RFC 791). IPv4 has proven to be robust, easily implemented, and interoperable. It has stood the test of scaling an internetwork to a global utility the size of today's Internet, which is a tribute to its initial design.

The initial design, however, did not anticipate the exponential growth of the Internet and the exhaustion of the IPv4 address space, or the effort required to maintain routing information. Because of the way in which IPv4 network IDs are allocated, there are routinely over 70,000 routes in the routing tables of Internet backbone routers. Most current IPv4 implementations are configured either manually or through a stateful address configuration protocol such as Dynamic Host Configuration Protocol (DHCP). With more computers and devices using IP, there is a need for a simpler and more automatic configuration of addresses and other configuration settings that do not rely on the administration of a DHCP infrastructure.

Another factor driving the development of IPv6 is the need for improved encryption. Private communication over a public medium like the Internet requires encryption services that protect the data sent from being viewed or modified in transit. There is a standard for providing security for IPv4 packets (known as Internet Protocol security or IPSec). In IPv4, however, this standard is optional and proprietary solutions are prevalent.

While standards for quality of service (QoS) exist for IPv4, real-time traffic support relies on the IPv4 Type of Service (TOS) field and the identification of the payload, typically using a User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) port. Unfortunately, the IPv4 TOS field has limited functionality and has different interpretations. In addition, payload identification using a TCP or UDP port is not possible when the IPv4 packet payload is encrypted.

To address these concerns, the IETF has developed a suite of protocols and standards known as IP version 6 (IPv6). This new version, previously named IP-The Next Generation (IPng), incorporates the concepts of many proposed methods for updating the IPv4 protocol. IPv6 is intentionally designed for minimal impact on upper and lower layer protocols by avoiding the arbitrary addition of new features.

For the latest set of RFCs and Internet drafts describing IPv6/IPv4 coexistence and migration technologies, see the Next Generation Transition (ngtrans) Working Group Web site at:

www.ietf.org/html.charters/ngtrans-charter.html

(Web addresses can change, so you might be unable to connect to the Web site or sites mentioned here.)

Benefits and purposes of the IPv6 protocol

The IPv6 header has a new format that is designed to minimize header validation and processing. An IPv6 address is four times larger than an IPv4 address. The global addresses used on the IPv6 portion of the Internet are designed to create an efficient, hierarchical, and summarized routing infrastructure that addresses the common occurrence of multiple levels of Internet service providers. On the IPv6 Internet, the backbone routers have an efficient and hierarchical addressing and routing infrastructure that uses smaller routing tables.

IPv6 supports both stateful address configuration, such as address configuration in the presence of a DHCP server, and stateless address configuration, or address configuration in the absence of a DHCP server. The support for IPSec is an IPv6 protocol suite requirement. This requirement provides a standards-based solution for network security needs and promotes interoperability between different IPv6 implementations. The new fields in the IPv6 header define how traffic is handled and identified.

Traffic identification, by using a Flow Label field in the IPv6 header, allows routers to identify and provide special handling for packets that belong to a flow. (A flow is a series of packets between a source and destination.) Because the traffic is identified in the IPv6 header, support for quality of service (QoS) can be easily achieved even when the packet payload is encrypted with IPSec.

The new Neighbor Discovery protocol for neighboring node interaction in IPv6 is a series of messages from the Internet Control Message Protocol for IPv6 (ICMPv6) that manage the interaction of neighboring nodes. Neighbor Discovery replaces Address Resolution Protocol (ARP), ICMPv4 Router Discovery, and ICMPv4 Redirect messages with efficient multicast and unicast messages.

IPv6 can be extended for new features by adding extension headers after the IPv6 header. Unlike the IPv4 header, which can only support 40 bytes of options, the size of IPv6 extension headers is only constrained by the size of the IPv6 packet. The following table compares the key features of the IPv4 and IPv6 protocols.

Comparison of features in IPv4 and IPv6

IPv4	IPv6
Source and destination addresses are 32 bits (4 bytes) in length.	Source and destination addresses are 128 bits (16 bytes) in length.
IPsec support is optional.	IPsec support is required.
No identification of packet flow for QoS handling by routers is present within the IPv4 header.	Packet flow identification for QoS handling by routers is included in the IPv6 header using the Flow Label field.
Fragmentation is done by both routers and the sending host.	Fragmentation is not done by routers, only by the sending host.
Header includes a checksum.	Header does not include a checksum.
Header includes options.	All optional data is moved to IPv6 extension headers.
Address Resolution Protocol (ARP) uses broadcast ARP Request frames to resolve an IPv4 address to a link layer address.	ARP Request frames are replaced with multicast Neighbor Solicitation messages.
Internet Group Management Protocol (IGMP) is used to manage local subnet group membership.	IGMP is replaced with Multicast Listener Discovery (MLD) messages.
ICMP Router Discovery is used to determine the IPv4 address of the best default gateway and is optional.	ICMP Router Discovery is replaced with ICMPv6 Router Solicitation and Router Advertisement messages and is required.

Broadcast addresses are used to send traffic to all nodes on a subnet.	There are no IPv6 broadcast addresses. Instead, a link-local scope all-nodes multicast address is used.
Must be configured either manually or through DHCP.	Does not require manual configuration or DHCP.
Uses host address (A) resource records in the Domain Name System (DNS) to map host names to IPv4 addresses.	Uses host address (AAAA) resource records in the Domain Name System (DNS) to map host names to IPv6 addresses.
Uses pointer (PTR) resource records in the IN-ADDR.ARPA DNS domain to map IPv4 addresses to host names.	Uses pointer (PTR) resource records in the IP6.INT DNS domain to map IPv6 addresses to host names.
Must support a 576-byte packet size (possibly fragmented).	Must support a 1280-byte packet size (without fragmentation).

For more information about IP version 6, see the Microsoft Web site at:

www.microsoft.com/windowsserver2003/technologies/ipv6/

Overview: Using the IPv6 protocol in a non-native IPv6 environment

On networks that do not have native support for IPv6 traffic, the IPv6 traffic is transmitted on the network by encapsulating the IPv6 packets within IPv4 packet headers. One such method of transmission is referred to as 6to4 tunneling.

For more information about the 6to4 tunneling technique, see "Connection of IPv6 Domains via IPv4 Clouds" in RFC 3056 on the Internet Engineering Task Force (IETF) Web site at:

www.ietf.org/rfc/rfc3056.txt?number=3056/

(Web addresses can change, so you might be unable to connect to the Web site or sites mentioned here.)

How the IPv6 protocol communicates with sites on the Internet

Although there are differences between the two protocol versions IPv4 and IPv6, their differences do not prevent them from coexisting or communicating on the IPv4 network.

If native IPv6 connectivity does not exist, a computer makes a Domain Name System (DNS) query for network relay routers that provide IPv6 service as part of the startup process. By default, this DNS query is presently set to "6to4.ipv6.microsoft.com" and the response contains a well-known IPv4 anycast address. (An anycast address is one that identifies multiple nodes and interfaces.) As more IPv6 relay routers are added in the future, this address will be assigned to more computers that are owned by various Internet service providers (ISPs).

If the DNS query provides multiple addresses, the host selects an appropriate relay router by sending an IPv6 packet to each one and choosing the one that responds first.

> **Note** 6to4 tunneling is enabled when IPv6 services are not native to your network and there is a public IPv4 Internet address present on the network access point.

The use of IPv6 in Microsoft Windows XP Professional Service Pack 1 (SP1) is currently supported only when IPv4 is also installed.

Security information for IPv6

TCP/IP networks are susceptible to a variety of possible attacks, from passive attacks (such as eavesdropping) to active attacks (such as denial-of-service attacks). For more information about general security issues with IP, especially in a large organization, see "Best Practices for Enterprise Security" on the Microsoft Web site at:

www.microsoft.com/technet/security/bestprac/bpent/bpentsec.asp

Controlling the IPv6 protocol to limit the flow of information to and from the Internet

You can stop the ingress or egress of IPv6 traffic on your network by configuring your network firewall to block all IPv6-specific packets. When the 6to4 tunneling technique is used, you can configure your firewall to block all IPv4 packets that include the IPv6 protocol designation of 41 in the protocol field of the IPv4 packet header.

The default settings for a member of the computer users group do not permit those users to install networking protocols. You should limit who is allowed to install the IPv6 stack on network computers by carefully limiting the number of users that have administrative logon credentials.

You can use the Active Directory directory service and Group Policy to filter and control the user’s ability to add new networking protocols, or to modify existing networking configurations. For more information about these configuration methods, see "Group Policy" in the Windows Help index. For information about installing and uninstalling IPv6, see the list of procedures in the next subsection.

Procedures for configuration of the IPv6 protocol

Installing and uninstalling the IPv6 protocol stack can be done by using the Network Connections folder or the command prompt.

The following two procedures describe installing and uninstalling the IPv6 protocol stack by using the Network Connections folder.

To install IPv6 using the Network Connections folder

1. Open **Network Connections**.
2. Right-click any local area connection, and then click **Properties**.
3. Click **Install**.
4. In the **Select Network Component Type** dialog box, click **Protocol**, and then click **Add**.
5. In the **Select Network Protocol** dialog box, click **Microsoft TCP/IP version 6**.
6. Click **Close** to save changes to your network connection.

To uninstall IPv6 using the Network Connections folder

1. Open **Network Connections**.
2. Right-click any local area connection, and then click **Properties**.

3. Click **Microsoft TCP/IP version 6** in the list of installed components, and then click **Uninstall**.
4. In the **Uninstall Microsoft TCP/IP version 6** dialog box, click **Yes**.
5. Click **Close** to save changes to your network connection.

Note To open Network Connections, click **Start**, click **Settings**, and then click **Network Connections**.

The following two procedures describe installing and uninstalling the IPv6 protocol stack by using the command prompt.

To install IPv6 on a computer using the command prompt

1. Open **Command Prompt**.
2. At the command prompt, type **ipv6 install**, and then press ENTER.

To uninstall IPv6 from a computer using the command prompt

1. Open **Command Prompt**.
2. At the command prompt, type **ipv6 uninstall**, and then press ENTER.

Notes
To open the command prompt, click **Start**, point to **All Programs**, point to **Accessories**, and then click **Command Prompt**.

The IPv6 configuration options require that you have administrative credentials on the computer.

Monitoring and troubleshooting the IPv6 protocol

Use the Internet protocol command-line prompt to view the TCP/IP configurations associated with a computer.

To display the complete list of TCP/IP interface configurations for a computer using the command prompt

1. Open **Command Prompt**.
2. At the command prompt, type **ipconfig /all**, and then press ENTER.

To display the TCP/IP routing table using the command prompt

1. Open **Command Prompt**.
2. At the command prompt, type **route print**, and then press ENTER.

Note For more information about TCP/IP configurations, see "TCP/IP utilities" in the Windows Help index.

Troubleshooting a command-line installation error

The installation of the IPv6 protocol stack requires that you have administrative credentials. The command-line prompt will yield the "Access is denied" error (0x800700005) if you attempt to install the IPv6 protocol from the command-line prompt without having the required account credentials.

Related Links

Web resources

- For more information about the 6to4 tunneling technique, see "Connection of IPv6 Domains via IPv4 Clouds" in RFC 3056 on the IETF Web site at:

  www.ietf.org/rfc/rfc3056.txt?number=3056/

  (Web addresses can change, so you might be unable to connect to the Web site or sites mentioned here.)

- For more information about IP version 6, see the Microsoft Web site at:

  www.microsoft.com/windowsserver2003/technologies/ipv6/

- For more information about enterprise security, see "Best Practices for Enterprise Security" on the Microsoft Web site at:

  www.microsoft.com/technet/security/bestprac/bpent/bpentsec.asp

- For more information about IPv6 addressing, see "IP Version 6 Addressing Architecture" in RFC 2373 on the IETF Web site at:

  www.ietf.org/rfc/rfc2373.txt?number=2373/

  (Web addresses can change, so you might be unable to connect to the Web site or sites mentioned here.)

- For the latest set of RFCs and Internet drafts describing IPv6/IPv4 coexistence and migration technologies, see the Next Generation Transition (ngtrans) Working Group Web site at:

  www.ietf.org/html.charters/ngtrans-charter.html

  (Web addresses can change, so you might be unable to connect to the Web site or sites mentioned here.)

Printed references

For more information about the IPv6 protocol suite, you can consult the following references:

- Davies, J. *Understanding IPv6.* Redmond, WA: Microsoft Press, 2002.
- Huitema, C. *IPv6: The New Internet Protocol.* Second edition. Upper Saddle River, NJ: Prentice Hall, 1998.
- Miller, M. *Implementing IPv6*: *Supporting the Next Generation of Protocols*. Second edition. Foster City, CA: M&T Books, 2000.

MSN Explorer

The following sections provide information about:

- The benefits of MSN® Explorer
- How MSN Explorer communicates with sites on the Internet
- How to control MSN Explorer to limit the flow of information to and from the Internet

Benefits and purposes of MSN Explorer

MSN Explorer is a feature that connects the user to the free non-subscriber section of the MSN.com Web site. From this default site the user has access to all of the MSN services. The MSN.com Web site is an Internet connectivity service that provides access to a variety of personal-interest information and services, as well as providing a portal to the World Wide Web.

Overview: Using MSN Explorer in a managed environment

MSN Explorer is installed optionally with Microsoft Windows XP Professional Service Pack 1 (SP1) and is available to users after completing a sign-up procedure through MSN Explorer Wizard. Once users have established an account with MSN.com they have access to personal e-mail, online contacts, online music and video, and the Internet. MSN Explorer delivers the benefits of popular Internet technologies such as hotmail, Microsoft Internet Explorer, Windows Messenger, and Windows Media Player, all in one program that works with the existing Internet connections. In a managed environment, however, unlimited access to these available Web sites may pose security risks. You can therefore remove MSN Explorer from the Windows components during installation as described later in this section.

How MSN Explorer communicates with sites on the Internet

The MSN Explorer component is a Web browser that can create an Internet connection, search the Web, communicate through instant messaging and e-mail, play music, and manage the users' schedules and finances online.

To access MSN Explorer, users must click Start, point to Programs, and then click MSN Explorer. The first time users access MSN Explorer, a dialog box opens on the desktop that asks if they would like to get on the Internet and write e-mail through the Start menu using MSN Explorer. By selecting either Yes or No, a Welcome to MSN Explorer Wizard opens that takes users through a sign-up process. Users have the option of signing up for MSN Internet Access with an MSN dial-up account, an existing Internet account, or an access method such as a local area network (LAN). Users then have the option of using an existing hotmail or MSN e-mail account or creating a new account. If they create a new e-mail account the wizard requests personal information such as date of birth and occupation. They then set a password and are given their user name. Subsequent access to MSN Explorer will take them directly to MSN.com.

This section describes various aspects of the data that is sent to and from the Internet, and how the exchange of information takes place.

- **Specific information sent or received**: MSN collects personal information such as e-mail address, name, home or work address, and telephone number. MSN also collects demographic information, such as ZIP Code, age, gender, preferences, interests, and favorites. Information about the computer hardware and software is also collected. This information may include: IP address, browser type, domain names, access times, and referring Web site addresses. MSN uses .NET Passport to provide registration and sign-in services. All of the registration information provided is stored by MSN, and some or all of that information will also be stored by .NET Passport.

- **Default target**: MSN.com is the target Internet Web site.
- **Triggers**: The user must choose to go to MSN.com by clicking the MSN Explorer icon.
- **Logging**: The information collected is logged and stored by MSN, .NET Passport, or both.
- **Access**: MSN and its operational service partners collect and use the personal information collected to operate MSN effectively and to deliver the services that the user has requested. Some information is also sent to MSN servers for service quality monitoring and the AutoUpdate service. For more information about how the information that is collected is used, see the MSN privacy policy at privacy.msn.com/.
- **Privacy policy**: There is a privacy statement for MSN Explorer. MSN also has a privacy statement that applies to the Microsoft MSN family of Web sites and governs data collection and usage at all MSN sites and services.
- **Transmission protocol and port**: The transmission protocol is HTTP and the port is 80.
- **Ability to disable**: MSN Explorer can be removed during installation as explained in "Procedures for configuration of MSN Explorer" later in this section.

Controlling MSN Explorer to limit the flow of information to and from the Internet

The MSN Explorer component can be disabled optionally when installing the operating system through the use of an answer file during unattended installation. The administrator also has the option of using Group Policy to block users from running MSN Explorer if it is already installed. Typically administrators will deploy firewalls, Network Address Translation (NAT) components, or both on their networks. They can block direct access to the MSN.com Web site at the firewall or gateway server as determined by the organization’s Internet use security policies. The following subsection provides procedures for configuring MSN Explorer to limit the flow of information to the Internet through an answer file during unattended installation and through Group Policy.

Procedures for configuration of MSN Explorer

MSN Explorer can be configured in several ways as described previously. This subsection describes the procedures to disable this component in accordance with your company’s security policies.

The following procedures explain how to:

- Exclude the MSN Explorer component during unattended installation of Windows XP SP1 by using an answer file.
- Use Group Policy to prevent users from running MSN Explorer if the component is already installed.

To exclude the MSN Explorer component during unattended installation by using an answer file

1. Using the methods you prefer for unattended installation or remote installation, create an answer file. For more information about unattended and remote installation, see Appendix A, "Resources for

learning about automated installation and deployment." Do not perform this procedure, however, if you are using Winbom.ini or Unattend.txt for your answer file.

2. In the [Components] section of the answer file, include the following entry:

   Msnexplr = Off

   Notes
   Do not set Msnexplr equal to No in the [Components] section of Winbom.ini or Unattend.txt.

   You can also check a registry key (manually or with a script) on a computer running Windows XP SP1 to see whether the games component is installed. Do not, however, change this registry key. A registry key value of 0x00000000 means the component is not installed, and a value of 0x00000001 means the component is installed. The key is as follows:

   HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\OC Manager\Subcomponents\msnexplr

To use Group Policy to block access to MSN Explorer

1. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.
   For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for learning about Group Policy."
2. Click **User Configuration**, click **Administrative Templates**, and then click **System**.

   Note There is no direct option to block access to MSN Explorer; however, you can add it to the list of applications that users are excluded from using, as described in the remaining steps in this procedure.

3. In the details pane, double-click **Don’t run specified Windows applications**.
4. Select **Enabled**, click **Show**, click **Add**, and then enter the application executable name (msn6.exe).

NetMeeting

The following sections provide information about:

- The benefits of NetMeeting
- Using NetMeeting in a managed environment
- How NetMeeting communicates with sites on the Internet
- How to control NetMeeting to limit the flow of information to and from the Internet

Benefits and purposes of NetMeeting

NetMeeting® conferencing software is a feature of Windows XP Professional Service Pack 1 (SP1) that enables real-time communication and collaboration over the Internet or an intranet. From a computer running the Windows 95, Windows 98, Windows NT 4.0, Windows 2000, or Windows XP operating system, users can communicate over a network with real-time voice and video technology. Users can work together on virtually any Windows-based application, exchange or mark up graphics on an electronic whiteboard, transfer files, or use the text-based chat program.

NetMeeting helps small and large organizations take full advantage of their corporate intranet for real-time communications and collaboration. On the Internet, connecting to other NetMeeting users is made easy with Internet Locator Service (ILS), enabling participants to call each other from a dynamic directory within NetMeeting or from a Web page. New features include remote desktop sharing, virtual conferencing using Microsoft Outlook, new security features, and the ability to embed the NetMeeting user interface in an organization's intranet Web pages.

To learn more about the NetMeeting features, see the article on the Microsoft TechNet Web site at:

www.microsoft.com/technet/prodtechnol/netmting/evaluate/nm3feats.asp

Overview: Using NetMeeting in a managed environment

NetMeeting supports communication standards for audio, video, and data conferencing. NetMeeting users can communicate and collaborate with users of other standards-based, compatible products. They can connect by modem, Integrated Services Digital Network (ISDN), or local area network (LAN) using Transmission Control Protocol/Internet Protocol (TCP/IP). In addition, support for Group Policy in NetMeeting makes it easy for administrators to centrally control and manage the NetMeeting work environment.

You can use Active Directory directory service and Group Policy to configure NetMeeting to meet your security requirements. You can also control the configuration of NetMeeting by using the NetMeeting Resource Kit. For more information, see "Alternate methods for controlling NetMeeting," later in this section.

NetMeeting components and features require that several ports be open from the firewall. For more information, see "NetMeeting and firewalls" later in this section.

How NetMeeting communicates with sites on the Internet

NetMeeting provides an infrastructure for communication between network applications and services. In this infrastructure, NetMeeting is both an application and a platform for other applications or services. The components and services in NetMeeting provide real-time communication and collaboration over the Internet or an organization's intranet.

NetMeeting audio and video conferencing features are based on the H.323 infrastructure, which enables NetMeeting to interoperate with other H.323 standards-based products. (H.323 is a standard approved by the International Telecommunication Union [ITU] that defines how audiovisual conferencing data is transmitted across networks.) NetMeeting data conferencing features are based on the T.120 infrastructure, enabling NetMeeting to interoperate with other T.120 standards-based products. (The T.120 standard is a suite of communication and application protocols developed for real-time, multipoint data connections and conferencing.)

Detailed information about the H.323 and T.120 standards is beyond the scope of this paper. Further information can be found on the following sites:

- For more information about the H.323 standard and NetMeeting, see "Understanding the H.323 Standard" at:

  www.microsoft.com/technet/prodtechnol/netmting/reskit/netmtg3/part3/chaptr11.asp

- For more information about the H.323 specification, see the following Web sites at:

  www.itu.int/home/index.html

  www.imtc.org/h323.htm

  (Web addresses can change, so you might be unable to connect to the Web site or sites mentioned here.)

- To learn more about the T.120 standard and NetMeeting, see "Understanding the T.120 Standard" at:

  www.microsoft.com/technet/prodtechnol/netmting/reskit/netmtg3/part3/chaptr10.asp

- For more information about the T.120 architecture, see the International Multimedia Teleconferencing Consortium (IMTC) Web site at:

  www.imtc.org/

  (Web addresses can change, so you might be unable to connect to the Web site or sites mentioned here.)

NetMeeting port assignments

When you use NetMeeting to call other users over the Internet, several IP ports are required to establish the outbound connection. The following table describes the port numbers, their functions, and the resulting connection.

Port assignments for NetMeeting

Port	Function	Outbound connection
389	Internet Locator Service (ILS)	TCP
522	User Location Service (ULS)	TCP
1503	T.120	TCP
1720	H.323 call setup	TCP
1731	Audio call control	TCP

1024 through 65535 (dynamic)	H.323 call control	TCP
1024 through 65535 (dynamic)	H.323 streaming	Real-Time Transfer Protocol (RTP) over User Datagram Protocol (UDP)

For more information about NetMeeting communication ports and firewall configuration topics, see "Firewall Configuration" on the Microsoft Web site at:

www.microsoft.com/technet/prodtechnol/netmting/reskit/netmtg3/part2/chapter4.asp

Controlling NetMeeting to limit the flow of information to and from the Internet

You can configure NetMeeting by using Group Policy objects (GPOs) on servers running Windows 2000. (You can also control the configuration of NetMeeting by using the NetMeeting Resource Kit; for more information, see "Alternate methods for controlling NetMeeting," later in this section.)

This subsection includes information about the following topics:

- NetMeeting and Group Policy
- NetMeeting security
- NetMeeting and firewalls
- Establishing a NetMeeting connection with a firewall
- Firewall limitations for NetMeeting

NetMeeting and Group Policy

Group Policy can be used to define the default NetMeeting configuration settings that will be automatically applied to users and computers. These settings determine which NetMeeting features and capabilities are available to a particular group of users. The Group Policy configuration settings that are specific to NetMeeting are grouped into two different categories. These category groupings enable you to independently manage NetMeeting configuration settings for computers and users within your organization. Through the use of Group Policy you can enable, disable, or set configuration options for NetMeeting features or capabilities.

For additional information about Group Policy, see the following appendices in this white paper:

- Appendix B, "Resources for learning about Group Policy."
- Appendix C, "Importing Group Policy settings for Windows XP to a server running Windows 2000 SP3."

You can use Group Policy to manage the following NetMeeting configuration options for users in your organization:

- NetMeeting Group Policy settings for computers
- NetMeeting Group Policy settings for users

Configuring NetMeeting settings for computers through Group Policy

You can use Group Policy to determine the NetMeeting features and capabilities that are available to all users of the computers that are affected by the application of the NetMeeting Group Policy settings.

For details about locating the Group Policy objects (GPOs) for NetMeeting, see "Procedures for configuration of NetMeeting" later in this section. The NetMeeting Group Policy configuration setting that is specific to computers is as follows:

- **Disable remote Desktop Sharing**: You can use Group Policy to set remote desktop sharing choices in NetMeeting for the all users that are affected by the application of this Group Policy setting.

For more information about how to use Group Policy to manage the NetMeeting computer settings, see "To disable the NetMeeting remote Desktop sharing feature through Group Policy" later in this section.

Note Computer-related Group Policy settings are applied when the operating system is initialized and during the periodic refresh cycle.

Configuring NetMeeting settings through Group Policy

You can use Group Policy to determine the NetMeeting features and capabilities that are available for a user or a group of users that are affected by the application of the NetMeeting Group Policy settings.

These Group Policy configuration options include the policy settings for NetMeeting, application sharing, audio and video, and the options page.

For more information about how to use Group Policy to manage the NetMeeting user settings, see "To disable the NetMeeting advanced calling feature through Group Policy" and "To disable the NetMeeting chat feature through Group Policy" later in this section.

The NetMeeting Group Policy configuration settings that are specific to users are as follows:

Configuring NetMeeting settings for users through Group Policy

For details about locating the Group Policy objects for NetMeeting, see "Procedures for configuration of NetMeeting" later in this section. You can use Group Policy to set configuration settings for the following NetMeeting features:

- **Enable Automatic Configuration**: Configures NetMeeting to download settings for users each time it starts.
- **Disable Directory services**: Disables the directory feature—users will not log on to a directory server when NetMeeting starts. Users will not be able to view or make calls using the NetMeeting directory.
- **Prevent adding Directory servers**: Prevents the user from adding directory servers to the list of available directory servers they can use for placing calls.
- **Prevent viewing Web directory**: Prevents the user from viewing directories as Web pages in a browser.
- **Set the intranet support Web page**: Sets the Web address that NetMeeting will display when users choose the Online Support command from the NetMeeting Help menu.
- **Set Call Security options**: Sets the level of security for outgoing and incoming NetMeeting calls.
- **Prevent changing Call placement method**: Prevents the user from changing the way calls are placed, either directly or by means of a gatekeeper server.

- **Prevent automatic acceptance of Calls**: Prevents the user from turning on automatic acceptance of incoming calls.
- **Allow persisting automatic acceptance of Calls**: Sets automatic acceptance of incoming calls to be persistent.
- **Prevent sending files**: Prevents users from sending files to others in a conference.
- **Prevent receiving files**: Prevents users from receiving files from others in a conference.
- **Limit the size of sent files**: Sets the maximum file size that can be sent to others in a conference.
- **Disable Chat**: Disables the chat feature of NetMeeting.
- **Disable NetMeeting 2.x Whiteboard**: Disables the NetMeeting 2.x Whiteboard feature. (The 2.x feature provides compatibility with older versions of NetMeeting only.)
- **Disable Whiteboard**: Disables the whiteboard feature of NetMeeting.

Configuring NetMeeting Application Sharing settings through Group Policy

For details about locating the Group Policy objects (GPOs) for NetMeeting, see "Procedures for configuration of NetMeeting" later in this section. You can use Group Policy to set configuration settings for the following elements of the NetMeeting Application Sharing feature:

- **Disable application Sharing**: Disables the NetMeeting application sharing feature completely. Users will not be able to host or view shared applications.
- **Prevent Sharing**: Prevents the user from sharing anything themselves. They will still be able to view shared applications or desktops from others.
- **Prevent Desktop Sharing**: Prevents the users from sharing their Windows desktop. They will still be able to share individual applications.
- **Prevent Sharing Command Prompts**: Prevents the user from sharing command prompts. Enabling this prevents the user from inadvertently sharing applications, since command prompts can be used to start other applications.
- **Prevent Sharing Explorer windows**: Prevents the user from sharing Windows Explorer windows. Enabling this prevents the user from inadvertently sharing applications, since Explorer windows can be used to start other applications.
- **Prevent Control**: Prevents users from allowing others in a conference to control what they have shared. Enabling this enforces a read-only mode whereby the other participants cannot change the data in the shared application.
- **Prevent Application Sharing in true color**: Prevents users from sharing applications in true color, which uses more bandwidth.

Configuring NetMeeting audio and video settings through Group Policy

For details about locating the Group Policy objects (GPOs) for NetMeeting, see "Procedures for configuration of NetMeeting" later in this section. You can use Group Policy to set configuration settings for the following audio and video elements in NetMeeting:

- **Limit the bandwidth of Audio and Video**: Configures the maximum bandwidth, specified in kilobytes per second, to be used for audio and video.
- **Disable Audio**: Disables the audio feature of NetMeeting; users will not be able to send or receive audio.

- **Disable full duplex Audio**: Disables the full duplex audio mode. Users will not be able to listen to incoming audio while speaking into the microphone. Older audio hardware may not perform well when full duplex audio is enabled.
- **Prevent changing DirectSound Audio setting**: Prevents the user from changing the DirectSound audio setting. DirectSound has a better audio quality, although older audio hardware may not support it.
- **Prevent sending Video**: Prevents the user from sending video. Setting this option does not prevent the user from receiving video.
- **Prevent receiving Video**: Prevents the user from receiving video. Setting this option does not prevent the user from sending video.

Configuring NetMeeting Options settings through Group Policy

For details about locating the Group Policy objects (GPOs) for NetMeeting, see "Procedures for configuration of NetMeeting" later in this section. You can use Group Policy to set configuration settings for the following elements of the NetMeeting Options page:

- **Hide the General page**: Removes the General tab on the NetMeeting Options page.
- **Disable the Advanced Calling button**: Disables the Advanced Calling button from the General page.
- **Hide the Security page**: Removes the Security tab on the NetMeeting Options page.
- **Hide the Audio page**: Removes the Audio tab on the NetMeeting Options page.
- **Hide the Video page**: Removes the Video tab on the NetMeeting Options page.

Note User-related Group Policy settings are applied when a user logs on to the computer and during the periodic refresh cycle.

To learn about specific Group Policy settings that can be applied to computers running Windows XP Professional SP1, see the Windows XP Professional Resource Kit, Group Policy object settings spreadsheet at:

www.microsoft.com/WindowsXP/pro/techinfo/productdoc/gpss.asp

NetMeeting security

The NetMeeting security architecture for data conferencing takes advantage of the existing, standards-compliant security features of Windows XP SP1 and Microsoft Internet Explorer. The NetMeeting security architecture utilizes a 40-bit encryption technology and has the following security features:

- **Password protection**: This feature enables the user to create or participate in a meeting that requires a password to join. Password protection helps to ensure that only authorized users participate in a password-protected meeting. A password is also required to use the remote desktop sharing feature.
- **User authentication**: This feature provides a way to verify the identity of a caller or meeting participant using a personal or NetMeeting certificate.
- **Data encryption**: This feature helps to protect data exchanged during a meeting so that it is not easily read by any unauthorized parties that may intercept the data. The 40-bit data encryption applies to the whiteboard and chat features, shared applications, and transferred files. Audio and video communications are not encrypted.

NetMeeting security features integrate with security in Windows XP SP1 and Internet Explorer in the following ways:

- NetMeeting uses the NetMeeting private certificate store to provide personal certificates for user authentication and data encryption.
- NetMeeting uses the Windows certificate store to maintain NetMeeting certificates.
- NetMeeting uses the Crypto application programming interface (API) for certificate management and secure channels. (The Crypto API enables applications to encrypt or digitally sign data in a flexible manner while providing protection for private keys.)
- NetMeeting uses Security Support Provider Interface (SSPI) functions to generate and process security tokens.

These security features can be implemented by an administrator or a NetMeeting user. Using the NetMeeting Resource Kit Wizard or Group Policy in NetMeeting, the administrator can enforce security settings that apply to all users. If allowed by the administrator, NetMeeting users can also select their own security settings in the NetMeeting user interface (UI) and change security settings for individual calls.

You can use the following sources to learn more about NetMeeting configuration and security topics:

- For more information about the NetMeeting Resource Kit Wizard, see the Microsoft Web site at:

  www.microsoft.com/technet/prodtechnol/netmting/reskit/netmtg3/part2/chapter2.asp

- For more information about Kerberos authentication, see "The Kerberos Network Authentication Service (V5)" (RFC 1510) on the IETF Web site at:

  www.ietf.org/rfc/rfc1510.txt

  (Web addresses can change, so you might be unable to connect to the Web site or sites mentioned here.)

- For more information about the security features available in NetMeeting, see the Microsoft Web site at:

  www.microsoft.com/technet/prodtechnol/netmting/reskit/netmtg3/part2/chapter5.asp

NetMeeting and firewalls

You can configure firewall components in a variety of ways, depending on your organization's specific security policies and overall operations. While most firewalls are capable of allowing primary (initial) and secondary (subsequent) Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) connections, it is possible that they are configured to support only specific connections based on security considerations. For example, some firewalls support only primary TCP connections, which some professionals view as the most reliable.

For NetMeeting multipoint data conferencing—program sharing, whiteboard, chat, file transfer, and directory access—your firewall only needs to pass through primary TCP connections on assigned ports. NetMeeting audio and video features require secondary TCP and UDP connections on dynamically assigned ports.

Note NetMeeting audio and video features require secondary TCP and UDP connections. Therefore, when you establish connections through firewalls that accept only primary TCP connections, you are not able to use the audio or video features of NetMeeting.

Detailed firewall configuration procedures for NetMeeting are beyond the scope of this paper. For more information about NetMeeting firewall connections, see "Establishing a NetMeeting Connection with a Firewall" on the Microsoft Web site at:

www.microsoft.com/technet/prodtechnol/netmting/reskit/netmtg3/part2/chapter4.asp

Microsoft NetMeeting can be configured to work with an organization's existing firewall security. Because of limitations in most firewall technology, however, few products are available that enable you to securely transport inbound and outbound NetMeeting calls containing audio, video, and data across a firewall. You should consider carefully the relative security risks of enabling different parts of a NetMeeting call in your firewall product. You must especially consider the security risks involved when modifying your firewall configuration to enable any component of an inbound NetMeeting call.

Some organizations have security or policy concerns that require them to limit how fully they support NetMeeting in their firewall configuration. These concerns are based on network capacity planning or weaknesses in the firewall technology being used. For example, security concerns might prohibit an organization from accepting any inbound or outbound flow of UDP data through the firewall. Because these UDP connections are required for NetMeeting audio and video features, disabling this function excludes audio and video features in NetMeeting for calls through the firewall. The organization can still use NetMeeting data conferencing features such as program sharing, file transfer, whiteboard, and chat for calls through the firewall by allowing only TCP connections on ports 522 and 1503.

For more information about NetMeeting firewall security, see "Security and Policy Concerns" on the Microsoft Web site at:

www.microsoft.com/technet/prodtechnol/netmting/reskit/netmtg3/part2/chapter4.asp

Establishing a NetMeeting connection with a firewall

When you use NetMeeting to call other users over the Internet, several IP ports are required to establish the outbound connection.

If you use a firewall to connect to the Internet, it must be configured so that the following IP ports are not blocked:

- TCP ports 389, 522, 1503, 1720, and 1731
- TCP and UDP ports (1024 through 65535)

To establish outbound NetMeeting connections through a firewall, the firewall must be configured to do the following:

- Pass through primary TCP connections on ports 389, 522, 1503, 1720, and 1731.
- Pass through secondary TCP and UDP connections on dynamically assigned ports (1024 through 65535).

The H.323 call setup protocol dynamically negotiates a TCP port for use by the H.323 call control protocol. Also, both the audio call control protocol and the H.323 call setup protocol dynamically negotiate UDP ports for use by the H.323 streaming protocol, called the Real-Time Transfer Protocol (RTP). In NetMeeting, two UDP ports are designated on each side of the firewall for audio and video streaming, for a total of four ports for inbound and outbound audio and video. These dynamically negotiated ports are selected arbitrarily from all ports that can be assigned dynamically.

NetMeeting directory services require either port 389 or port 522, depending on the type of server you are using. The Microsoft Internet Locator Service (ILS), which supports LDAP for NetMeeting, requires port 389. The Microsoft User Location Service (ULS), developed for NetMeeting 1.0, requires port 522.

Firewall limitations for NetMeeting

Some firewalls cannot support an arbitrary number of virtual internal IP addresses, or cannot do so dynamically. With these firewalls, you can establish outbound NetMeeting connections from computers inside the firewall to computers outside the firewall, and you can use the audio and video features of NetMeeting. Users outside the organization cannot, however, establish inbound connections from outside the firewall to computers inside the firewall. Typically, this restriction is due to limitations in the network implementation of the firewall.

Note Some firewalls are capable of accepting only certain protocols and cannot handle TCP connections. For example, if your firewall is a Web proxy server with no generic connection-handling mechanism, you will not be able to use NetMeeting through the firewall.

You can use the following sources to learn more about NetMeeting configuration and firewall topics:

- For more information about NetMeeting firewall connections, see "Establishing a NetMeeting Connection with a Firewall" on the Microsoft Web site at:

  www.microsoft.com/technet/prodtechnol/netmting/reskit/netmtg3/part2/chapter4.asp

- For more information about using NetMeeting and your firewall, see "How to Establish NetMeeting Connections through a Firewall" on the Microsoft Web site at:

  support.microsoft.com/default.aspx?scid=KB;en-us;Q158623

Alternate methods for controlling NetMeeting

You can create customized installation options for specific users or groups within your organization by using the NetMeeting Resource Kit Wizard. Additionally, you can use the NetMeeting Resource Kit Wizard to control user and computer access rights by creating custom configurations of client settings and specific features that you have selected to restrict or allow. For example, you can control audio and video access, set data throughput limits and network speeds, and choose to display online support. The Resource Kit Wizard can also help you set up various configurations of NetMeeting for different types of users and different levels of security. It can help you save network bandwidth by restricting specific features. You can also use the Resource Kit Wizard to both change registry settings for all NetMeeting users, and implement such changes globally.

Note By selecting certain options in the Resource Kit Wizard, be aware that you may be changing the NetMeeting user interface. For example, if you click **Restrict the Use of Video**, the Video tab doesn't appear in the NetMeeting user's Options dialog box.

In addition, the Resource Kit for NetMeeting has a section that provides detailed information for responding to NetMeeting problems, including problem descriptions, causes, and resolutions.

For more information about the NetMeeting 3 Resource Kit, see Windows NetMeeting 3 Resource Kit on the Microsoft Web site at:

www.microsoft.com/technet/prodtechnol/netmting/reskit/netmtg3/nm3dldoc.asp

Procedures for configuration of NetMeeting

NetMeeting is designed to enhance the enterprise environment and enable users to communicate internally and externally with other NetMeeting users. You can use Group Policy to develop a NetMeeting feature management policy to support the specific business rules or communication policies that exist within your organization. For example, your organization may not want users to be able to access or use the NetMeeting chat feature from their computers. By using Active Directory and Group Policy, you can disable the chat feature from any or all computers that are affected by the application of the Group Policy configuration settings.

For lists of Group Policy settings that you can use to manage NetMeeting configuration options, see "NetMeeting and Group Policy" earlier in this section.

Procedures for managing NetMeeting features through Group Policy

This subsection provides procedures for the following configuration methods:

- Locating the Group Policy objects (GPOs) for NetMeeting configuration settings. These are the settings listed in "NetMeeting and Group Policy" earlier in this section.
- Disabling the NetMeeting remote desktop sharing feature.
- Disabling the NetMeeting advanced calling feature.
- Disabling the NetMeeting chat feature.

To locate the Group Policy objects (GPOs) for NetMeeting user configuration settings

1. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.
   For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for learning about Group Policy."
2. Click **User Configuration**, click **Administrative Templates**, click **Windows Components**, and then click **NetMeeting**.
3. View the Group Policy objects that are available. For more information about these objects, see "NetMeeting and Group Policy" earlier in this section.

Formatted: Bullets and Numbering

To locate the Group Policy objects (GPOs) for NetMeeting computer configuration settings

1. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.
   For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for learning about Group Policy."
2. Click **Computer Configuration**, click **Administrative Templates**, click **Windows Components**, and then click **NetMeeting**.
3. View the Group Policy objects that are available. For more information about these objects, see "NetMeeting and Group Policy" earlier in this section.

Formatted: Bullets and Numbering

Use the following steps to configure the Group Policy setting to prevent users from using the NetMeeting remote desktop sharing feature:

To disable the NetMeeting remote Desktop sharing feature through Group Policy

1. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.
   For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for learning about Group Policy."
2. Click **Computer Configuration**, click **Administrative Templates**, click **Windows Components**, and then click **NetMeeting**.
3. In the details pane, double-click **Disable remote Desktop Sharing**.
4. Select **Enabled**.

Formatted: Bullets and Numbering

Note Computer-related Group Policy settings are applied when the operating system is initialized and during the periodic refresh cycle.

Use the following steps to configure the Group Policy setting to disable the advanced calling feature on the NetMeeting options page.

To disable the NetMeeting advanced calling feature through Group Policy

1. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.
   For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for learning about Group Policy."
2. Click **User Configuration**, click **Administrative Templates**, click **Windows Components**, click **NetMeeting**, and then click **Options Page**.
3. In the details pane, double-click **Disable the Advanced Calling button**, and then select **Enabled.**

Formatted: Bullets and Numbering

Use the following steps to configure the Group Policy setting to prevent the use of the NetMeeting Chat feature.

To disable the NetMeeting chat feature through Group Policy

1. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.
   For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for learning about Group Policy."
2. Click **User Configuration**, click **Administrative Templates**, click **Windows Components**, and then click **NetMeeting**.
3. In the details pane, double-click **Disable Chat**, and then select **Enabled**.

Formatted: Bullets and Numbering

Related Links

Web resources

- For more information on using NetMeeting and your firewall, see "How to Establish NetMeeting Connections through a Firewall" on the Microsoft Web site at:

  support.microsoft.com/default.aspx?scid=KB;en-us;Q158623

- For more information about NetMeeting, see Windows NetMeeting on the Microsoft Web site at:

  www.microsoft.com/windows/NetMeeting/

- For more information on configuring NetMeeting, see the Windows NetMeeting Resource Kit on the Microsoft Web site at:

  www.microsoft.com/windows/NetMeeting/Corp/ResKit/

- To learn more about NetMeeting features, see the Microsoft Web site at:

  www.microsoft.com/technet/prodtechnol/netmting/evaluate/nm3feats.asp

- To view articles that explain how to use some of the new features in NetMeeting, see the Microsoft Web site at:

  support.microsoft.com/default.aspx?scid=/support/netmeeting/howto/default.asp

- For more information about Kerberos authentication, see "The Kerberos Network Authentication Service (V5)" (RFC 1510) on the Internet Engineering Task Force (IETF) Web site at:

  www.ietf.org/rfc/rfc1510.txt

- For more information about the H.323 specification, see the ITU-T Web site at:

  www.itu.int/home/index.html

- For more information about the T.120 architecture, see the International Multimedia Teleconferencing Consortium (IMTC) Web site at:

  www.imtc.org/

(Web addresses can change, so you might be unable to connect to the Web site or sites mentioned here.)

Printed references

For more information about firewall design, policy, and security considerations for firewall design in general, you can consult the following reference:

- Chapman, D. Brent and Elizabeth D. Zwicky. *Building Internet Firewalls*. O'Reilly & Associates, Inc., 1995.

Online Device Help

The following sections provide information about:

- The benefits of Online Device Help
- How Online Device Help communicates with sites on the Internet
- How to control Online Device Help to limit the flow of information to and from the Internet

Benefits and purposes of Online Device Help

Online Device Help (also known as the "Get help for my hardware device" wizard) delivers targeted content on problems with hardware and peripheral devices installed on the system. This mitigates the need for users to call support professionals to resolve hardware issues. Users interact with Online Device Help in Microsoft Windows XP Professional Service Pack 1 (SP1) when installing new hardware (through the Found New Hardware Wizard).

At the conclusion of the Found New Hardware Wizard, when the user's system uses a device driver that is not found on the Windows XP SP1 installation CD or is not available through Windows Update, Online Device Help collects anonymous data on the problem device (including a unique hardware identifier for that device) and sends that information over the Internet to a server at Microsoft. If a match for the device is found, content on that device is then downloaded to the user's system and is displayed in the Help and Support Center user interface. This content may include:

- Information from the independent hardware vendor (IHV) about upcoming and planned device support.
- Links to the product compatibility area in Help and Support Center to enable users to search or browse the Windows Catalog Web site for compatible devices. The Windows Catalog Web site is located at:

  www.microsoft.com/windows/catalog/
- A link to the Web site of the IHV for that device.

The data provided by Online Device Help enables Microsoft to identify the number and system locale of users experiencing hardware problems due to missing drivers and to identify the most common problem devices. Microsoft works with these hardware vendors to provide targeted troubleshooting content on the most common problem hardware devices.

This section of the white paper explains how to control Online Device Help in a managed environment.

Overview: Using Online Device Help in a managed environment

Users have control over whether to upload the data required by Online Device Help. In a managed environment, however, it is unlikely that users can choose to install any device; this function would normally be controlled in some fashion by the IT department. You can block Online Device Help at the firewall or through the Services snap-in. The configuration options and procedures for controlling Online Device Help are described later in this section.

How Online Device Help communicates with sites on the Internet

If no information for a particular hardware device is found on either the Windows XP installation CD or through Windows Update, the user is prompted to release anonymous information about their hardware profile through Online Device Help. This subsection summarizes the communication process:

- **Specific information sent or received:** The following information is collected from the user's computer and uploaded to a server at Microsoft. The user is not uniquely identified.
  - The hardware ID, also known as the PnPID (code that indicates the device manufacturer, device name, and version)
  - The time and date that the data was sent
  - Language code of the operating system, and platform and build information
- **Default and recommended settings**: Online Device Help is enabled by default. Recommended settings are described in the next subsection, "Controlling Online Device Help to limit the flow of information to and from the Internet."
- **Triggers**: Online Device Help is triggered if no information for a particular hardware device is found after the user has completed the Found New Hardware Wizard.
- **User notification**: Users are prompted to send anonymous hardware profile data to a server at Microsoft. If users opt to send this information, the privacy policy is displayed. Users can view the contents of the hardware.xml file being uploaded by clicking a link on the privacy policy page.
- **Logging**: Errors that result from problems installing hardware devices without drivers are logged to the event log.
- **Encryption**: The data transferred to Microsoft is not encrypted.
- **Access**: The raw data uploaded to the server is accessible to operations engineers at Microsoft.com and is used in the Windows Hardware Quality Labs (WHQL) to improve Windows-compatible hardware and drivers.
- **Privacy policy**: Online Device Help is covered by its own privacy policy. That policy (located in a file on the user's computer at %SystemRoot%\pchealth\helpctr\system\dfs\privacy.htm) is displayed when users opt to send the anonymous hardware profile data to Microsoft.
- **Transmission protocol and port**: The transmission protocol used is HTTP and the port is 80.
- **Ability to disable**: You cannot disable Online Device Help directly. Disabling Internet access or HTTP port 80 will, however, block Online Device Help.

Controlling Online Device Help to limit the flow of information to and from the Internet

Users have control over whether or not to upload anonymous hardware profile information about their system. You cannot, however, disable Online Device Help directly. To block Online Device Help, you can restrict Internet access. You can also use a firewall or configure the Services snap-in. The following table describes the result of each option.

Configuration settings for Online Device Help

Configuration tool	Setting	Result
Firewall	Block HTTP port 80.	Blocks Online Device Help.

Services snap-in	Disable the Upload Manager service (uploadmgr).	Blocks Online Device Help. Any other services that depend on uploadmgr will also fail to start.

How controlling Online Device Help can affect users and applications

If you decide to disable Online Device Help, users will not be prompted to upload anonymous hardware profile information and they will not receive up-to-date, targeted self-help content on hardware issues relating to missing or problem drivers.

> **Note** If you restrict Internet access to block Online Device Help, the feature will queue the data and periodically retry to upload the hardware profile information for some period of time. If an Internet connection becomes available during that period, Online Device Help will upload the queued data. If an Internet connection does not become available, no data will be uploaded. Users will not be impacted in either case.

Alternate methods for controlling Online Device Help

You can also control Online Device Help by disabling the Upload Manager service (uploadmgr) that manages synchronous and asynchronous file transfers between clients and servers on the network. Disabling this service will block the upload of the anonymous hardware profile data (although users will still be able to complete the Found New Hardware Wizard). The following subsection gives the procedure for this method.

Procedures for controlling Online Device Help

You cannot disable Online Device Help directly but can do so indirectly by disabling the Upload Manager service in Windows XP.

To disable Online Device Help by disabling the Upload Manager service

1. Click **Start**, and then either click **Control Panel**, or point to **Settings** and then click **Control Panel**. Double-click **Administrative Tools**, and then double-click **Services**.
2. In the details pane, right-click **Upload Manager**, and then click **Properties**.
3. Click the **Log On** tab, then click the hardware profile that you want to configure, and then click **Disable**.

> **Important** If the Upload Manager service is disabled, any services that explicitly depend on it will fail to start.

Outlook Express 6 SP1 (included in Internet Explorer 6 SP1)

The subsections that follow provide:

- A description of Microsoft Outlook Express 6 Service Pack 1 (SP1), which is included in Microsoft Internet Explorer 6 Service Pack 1 (SP1), and a comparison of Outlook and Outlook Express.
- Descriptions of new security-related features in Outlook Express 6 SP1 (as compared to Outlook Express 5), with information about how they are configured at the desktop.
- Information about removing all visible entry points to Outlook Express in Microsoft Windows XP Professional Service Pack 1 (SP1) (for situations where you want users to use another e-mail client exclusively). One way to do this is during unattended installation. Another way to do this is through Add or Remove Programs in Control Panel.
- Information about controlling Outlook Express 6 SP1 through Group Policy to limit the risk associated with e-mail attachments. The Group Policy setting you use for this is **Block attachments that could contain a virus**.

> **Notes**
> This section of the white paper describes Outlook Express 6 SP1, but does not describe Internet Explorer 6 (of which Outlook Express is part), the New Connection Wizard, or the tool that can report errors that occur in Outlook Express. For information about these components, see the respective sections of this white paper (the error reporting tool is described in "Windows Error Reporting").
>
> Also note that the New Connection Wizard replaces the Network Connection Wizard and the Internet Connection Wizard in Windows 2000.

It is beyond the scope of this white paper to describe all aspects of maintaining appropriate levels of security in an organization where users send e-mail, receive e-mail, open attachments in e-mail, and perform similar actions. This section, however, provides information about features and configuration methods in Outlook Express 6 SP1 that can reduce the inherent risks associated with sending and receiving e-mail.

For more information about Outlook Express, see the following resources:

- Help for Outlook Express (which can be accessed in Outlook Express by clicking the **Help** menu and then selecting an appropriate option).
- The section about Internet Explorer 6 SP1 in this white paper, which describes security zones in Internet Explorer 6 SP1. These security zones are also used in Outlook Express 6 SP1.
- The Internet Explorer page on the Microsoft Web site at:

  www.microsoft.com/windows/ie/
- The Resource Kit for Internet Explorer (specifically, the chapter describing what's new in Internet Explorer 6). To learn about this and other Resource Kits, see the Windows Deployment and Resource Kits Web site at:

  www.microsoft.com/reskit/

Benefits and purposes of Outlook Express 6 SP1

Outlook Express 6 SP1 is designed to make it easy to send or receive e-mail and to browse or participate in newsgroups. It differs from most of the other components described in this white paper in that its main function is to communicate through the Internet or an intranet (in contrast to components that communicate with the Internet in the process of supporting some other activity).

Outlook Express is part of Internet Explorer, in contrast to Microsoft Outlook, which is a program included in Microsoft Office. Outlook provides comprehensive integrated e-mail, including information management and collaboration capabilities, useful to a wide spectrum of users from home to small business to large enterprise. Outlook Express, included as part of Internet Explorer, offers standard Internet e-mail and news access, useful to many home and small-business users. Outlook Express supports Post Office Protocol 3 (POP3) or Internet Message Access Protocol (IMAP).

Outlook Express 6 SP1 offers more security-related options and settings than were available in Outlook Express 5. The following subsections describe the new options and ways of configuring them, as well as outlining a method for removing all visible entry points to Outlook Express in Windows XP SP1 (for situations where you want users to use another e-mail client exclusively).

New security-related features in Outlook Express 6 SP1

Outlook Express 6 SP1 is the e-mail component in Internet Explorer 6 SP1. This version of Outlook Express includes the following new security-related features. The table that follows this list shows how each option is configured in Outlook Express.

- **Warning about harmful e-mail**. To prevent e-mail messages from being sent without a user’s knowledge, Outlook Express warns the user when other programs, such as viruses or harmful attachments, attempt to send messages from the user’s computer. This warning appears only if Outlook Express is configured as the default simple MAPI client, and another program attempts to use simple MAPI to programmatically send e-mail messages without presenting a visible user interface on the computer.
- **Blocking of potentially harmful attachments**. If this option is enabled, Outlook Express 6 blocks the opening or saving of specific e-mail attachments that are considered "unsafe." To determine whether an attachment is unsafe, Outlook Express 6 uses the Internet Explorer 6 unsafe file list, plus some additional file types, plus file types you configure with the **Confirm open after download** setting in Folder Options (on the Files Types tab). Any e-mail attachment with a file type reported as "unsafe" is blocked. This option can be enabled or disabled through Group Policy as well as at the local computer. For more information about using this setting, see the table that follows and "To locate the Group Policy object (GPO) for blocking e-mail attachments in Outlook Express 6 SP1" later in this section.

  For information about the unsafe file list in Internet Explorer 6, you can search the Microsoft Knowledge Base. To do this, follow the instructions for searching on the Web site, and search for the phrase "unsafe file list":

  support.microsoft.com/
- **Software Restriction Policies technology**. When running with Windows XP, Outlook Express 6 SP1 takes advantage of Software Restriction Policies technology to run potentially harmful attachments in a sandbox, which is an area in memory outside of which the program cannot make calls. When a user attempts to run or save attachments, Software Restriction Policies technology determines whether the file formats are blocked. If so, Outlook Express displays a warning, and the program running the attachment has only limited access to the computer's hard disk and registry.
- **Plain text format option for reading of e-mail**. Starting with SP1 of Outlook Express 6, Outlook Express can be configured to read all e-mail messages in plain text format. Some HTML e-mail messages may not appear correctly in plain text, but no active content in the e-mail is run when this setting is enabled.

The following table shows how each option is configured in Outlook Express 6 SP1.

Options for configuring Outlook Express 6 SP1

Option to configure in Outlook Express 6 SP1	Menu to click	Menu item to click	Tab to click
Warning about harmful e-mail	Tools	Options	Security
Blocking of potentially harmful attachments (also configurable through Group Policy)	Tools	Options	Security
Software Restriction Policies technology	Tools	Options	Security
Plain text format option for reading of all e-mail	Tools	Options	Read (in SP1 only)

Overview: Using Outlook Express 6 SP1 in a managed environment

Although there are inherent risks associated with sending and receiving e-mail (and e-mail attachments), you can use a number of different features and configuration methods in Outlook Express 6 SP1 to reduce the risks:

- You can use the graphical user interface to configure the security-related features in Outlook Express 6 SP1. For more information, see "New security-related features in Outlook Express 6 SP1" earlier in this section and "To start Outlook Express 6 SP1 and view or configure security settings" later in this section.
- You can ensure that all visible entry points to Outlook Express in Windows XP SP1 are removed (for situations where you want users to use another e-mail client exclusively). For more information, see "Removing visible entry points to Outlook Express during deployment of Windows XP SP1" and "To remove visible entry points to Outlook Express on an individual computer running Windows XP SP1" later in this section.
- You can use a Group Policy setting, **Block attachments that could contain a virus,** to limit the risk associated with e-mail attachments in Outlook Express 6 SP1. For more information, see "To locate the Group Policy object (GPO) for blocking e-mail attachments in Outlook Express 6 SP1" later in this section.

Removing visible entry points to Outlook Express during deployment of Windows XP SP1

For situations where you always want users to use an e-mail client other than Outlook Express 6 SP1, you can remove all visible entry points to Outlook Express in Windows XP SP1. One way to do this is during workstation deployment by using standard methods for unattended installations or remote installations. If you are using an answer file, the entry is as follows:

```
[Components]
OEAccess = Off
```

For more information about unattended installation, see Appendix A, "Resources for learning about automated installation and deployment."

For information about removing all visible entry points to Outlook Express on an individual computer, see "To remove visible entry points to Outlook Express on an individual computer running Windows XP SP1," later in this section.

Procedures for working with Outlook Express 6 SP1

This section provides procedures for the following:

- Opening the dialog box from which you can configure security settings for Outlook Express 6 SP1.
- Locating the Group Policy setting, **Block attachments that could contain a virus**.

  You can use this Group Policy setting in situations where you want Outlook Express 6 SP1 to be available for users but where you want to limit the risk associated with e-mail attachments. For more information about this setting, see "New security-related features in Outlook Express 6 SP1" earlier in this section.
- Removing visible entry points to Outlook Express on an individual computer running Windows XP SP1.
- Removing visible entry points to Outlook Express during unattended installation of Windows XP SP1 by using an answer file.

To start Outlook Express 6 SP1 and view or configure security settings

1. Click **Start**, point to **All Programs** or **Programs**, and then click **Outlook Express**.
2. On the **Tools** menu, click **Options**.
3. Click the **Security** tab and view or configure the settings, including the check boxes for the following two options:
   - **Warn me when other applications try to send mail as me**.
   - **Do not allow attachments to be saved or opened that could potentially be a virus**.

   You can also view or configure the security zones setting. Outlook Express 6 SP1 uses two of the same security zones that you configure in Internet Explorer 6 SP1. For more information about security zones, see the section about Internet Explorer 6 SP1 in this white paper.
4. Click the **Read** tab, and view or configure the settings, including the check box for **Read all messages in plain text**.

To locate the Group Policy object (GPO) for blocking e-mail attachments in Outlook Express 6 SP1

1. Ensure that you have upgraded to the latest Administrative Template files. For more information, see Appendix C, "Importing Group Policy settings for Windows XP to a server running Windows 2000 SP3."
2. On a server running Window 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.

   For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for learning about Group Policy."
3. Click **User Configuration**, click **Administrative Templates**, click **Windows Components**, and then click **Internet Explorer**.

4. In the details pane, double-click **Configure Outlook Express**.
5. Select or clear the check box for **Block attachments that could contain a virus**.

To remove visible entry points to Outlook Express on an individual computer running Windows XP SP1

1. Click **Start**, and then either click **Control Panel**, or point to **Settings** and then click **Control Panel**.
2. Double-click **Add or Remove Programs**.
3. Click **Add/Remove Windows Components** (on the left).
4. Scroll down the list of components to Outlook Express, and make sure the check box for that component is cleared.
5. Follow the instructions to complete the Windows Components Wizard.

To remove visible entry points to Outlook Express during unattended installation by using an answer file

1. Using the methods you prefer for unattended installation or remote installation, create an answer file. For more information about unattended and remote installation, see Appendix A, "Resources for learning about automated installation and deployment."
2. In the [Components] section of the answer file, include the following entry:

   OEAccess = Off

Plug and Play

The following sections provide information about:

- The benefits of Plug and Play
- How Plug and Play communicates with sites on the Internet
- How to control Plug and Play to prevent the flow of information to and from the Internet

Benefits and purposes of Plug and Play

Windows Plug and Play provides ease of support for installing devices on computers in your network. You can simply plug in a Plug and Play device and Windows does the rest by installing any necessary drivers, updating the system, and allocating resources. After you install a Plug and Play device, the driver is configured and loaded dynamically, typically without requiring user input.

Plug and Play in Microsoft Windows XP Professional Service Pack 1 (SP1) provides the following services:

- Detects a Plug and Play device and determines its hardware resource requirements and device identification number (Plug and Play ID).
- Locates an appropriate device driver for newly installed devices.
- Allocates hardware resources.
- Dynamically loads, initializes, and unloads drivers.
- Notifies other drivers and applications when a new device is available.
- In conjunction with power management, handles stop and start processes for devices during hibernation, standby, and startup and shutdown operations.
- Supports a wide range of device types.

Overview: Using Plug and Play in a managed environment

The Plug and Play feature is enabled by default in Windows XP. When users install a Plug and Play device, and they are connected to the Internet, Windows XP automatically accesses Windows Update to search for a device driver.

> **Note** Some buses, such as Peripheral Component Interconnect (PCI) and universal serial bus (USB), take full advantage of Plug and Play. Older buses, such as Industry Standard Architecture (ISA), do not take full advantage of Plug and Play, and require more user interaction to ensure that devices are correctly installed.

If an administrator uses the Add Hardware Wizard to add new hardware that is not Plug and Play, Windows XP also provides limited Plug and Play support by accessing the Windows Update site to search for device drivers. Windows XP will, however, only access and use drivers signed by Microsoft Corporation. The same support is provided when an administrator uses the Found New Hardware and Hardware Update wizards. You must be logged on as an administrator or a member of the Administrators group in order to install devices using these wizards.

As an IT administrator in a highly managed network environment, you want to control the ability of users and administrators to install new hardware and to thereby access the Internet automatically when Windows XP searches for device drivers. For a more secure environment you can prevent users and administrators from installing hardware devices, or you can limit their ability to do so with Group Policy.

There are also policy settings you can use to disable Windows Update for all users, including other administrators. If you do prevent certain administrators from automatically accessing Windows Update, there is the option for manually downloading the updates from the Windows Update Catalog, whereby they can be distributed on your organization's network as needed.

Using Group Policy to disable access to Windows Update and configure driver search locations is described in the subsection "Controlling automatic device updating to prevent the flow of information to and from the Internet."

How Plug and Play communicates with sites on the Internet

There are three instances when a computer running Windows XP will access the Internet as part of Plug and Play:

- When Plug and Play searches for a driver for newly installed hardware
- When an administrator updates the driver for existing hardware
- When an administrator installs non-Plug and Play hardware using the Add Hardware Wizard

When you connect a new hardware device and there is no driver available on the computer, Windows XP will use the Windows Update service to search for available drivers on the Windows Update site. If an appropriate driver is found on the Windows Update site, Windows XP copies it and installs it on your computer. If your computer is not connected to the Internet, Windows XP displays a message prompting you to connect to the Internet.

As part of Plug and Play, when Windows XP searches for a device driver, interaction with the Internet takes place as follows:

- **Specific information sent or received**: The Code Download Manager (CDM) calls Windows Update to find and download device drivers. The CDM also calls Help and Support Center, which logs in Windows Update Plug and Play IDs for devices that Microsoft does not have drivers for. Neither of these communications is under the direct control of Plug and Play. The CDM handles all of the communication between the computer and Windows Update. None of the communication between the computer and the Internet uniquely identifies the user.
- **Default and recommended settings**: Plug and Play is enabled by default. Plug and Play cannot be disabled as system instability would result. Recommended settings are presented in the following subsection "Controlling automatic device updating to prevent the flow of information to and from the Internet."
- **Triggers**: When a user installs a Plug and Play device or an administrator adds hardware with any of the hardware wizards, Windows Update is automatically contacted for driver updates.
- **User notification**: When searching for a device driver Windows Update sends a list of available drivers to the user’s computer. Plug and Play ranks the drivers by signature, Plug and Play ID match, and the date of the driver package.
- **Logging**: If you use a Plug and Play driver with a non-Plug and Play device, any associated issues or problems are recorded in the event log.
- **Encryption**: Data transfer is based on interaction with Windows Update. The data is transferred using HTTPS.

- **Transmission protocol and ports:** The transmission protocols and ports are HTTP 80 and HTTPS 443.
- **Ability to disable**: You can limit features of Windows Update using Group Policy.

Controlling automatic device updating to prevent the flow of information to and from the Internet

Windows will automatically update device drivers using Plug and Play, and it will even search for compatible drivers for non-Plug and Play devices. You therefore might want to exercise various levels of control over users' and administrators' ability to install new hardware and to update hardware devices and drivers.

Using Group Policy there are several levels of control you can configure in order to prevent Plug and Play and associated hardware wizards from accessing the Internet. You can target search locations for drivers, or you can prevent users and computers from automatically accessing the Windows Update Web site in any instance. If you choose to disable automatic updating for users' computers, you can enable Windows Update for specified servers on your network, and have users' computers access an intranet server for selected updates.

You can use Group Policy to:

- Control whether Windows Update is included when Plug and Play searches for a device driver.

  This procedure is presented in the next subsection.
- Eliminate automatic update calls to Window Update.

  Policy settings related to automatic updating are at User Configuration\Administrative Templates\System.
- Remove access to Windows Update.

  When you enable the policy setting **Remove access to use all Windows Update features**, you block access to the Windows Update site from the Windows Update hyperlink on the Start menu and also on the Tools menu in Microsoft Internet Explorer. Windows automatic updating is also disabled; you will neither be notified about nor will you receive critical updates from Windows Update. This policy setting also prevents Device Manager from automatically installing driver updates from the Windows Update Web site.

  The Windows Update site is located at:

  windowsupdate.microsoft.com/

Policy settings related to Windows Update are at User Configuration\Administrative Templates\Windows Components\Windows Update.

Procedure for controlling where Plug and Play searches for drivers

When you install new hardware, Windows XP searches four different locations for drivers in the following order: the hard drive, the floppy drive, the CD-ROM drive, and Windows Update. The default approach is to search all four locations successively until the correct device driver is found; however, you can configure the driver search locations to remove any or all of these locations.

Included here is the procedure for configuring the Group Policy setting **Configure Driver Search Locations**. For additional procedures to configure policy settings for Windows Update, see the section "Windows Update and Automatic Update" in this white paper.

To disable Windows Update as a driver search location for Plug and Play devices

1. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.
   For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for learning about Group Policy."
2. Click **User Configuration**, click **Administrative Templates**, and then click **System**.
3. In the details pane, double-click **Configure Driver Search Locations**, and then select **Enabled**.
4. Select **Don’t Search Windows Update**.

Related Links

For more information about Windows Update, see:

windowsupdate.microsoft.com/

Program Compatibility Wizard

The following sections provide information about:

- The benefits of the Program Compatibility Wizard
- How the Program Compatibility Wizard communicates with sites on the Internet
- How to control the Program Compatibility Wizard to prevent the flow of information to the Internet

Benefits and purposes of the Program Compatibility Wizard

There are some applications that work on earlier versions of Windows that might fail to function properly on Microsoft Windows XP Professional Service Pack 1 (SP1). This can happen for several reasons—an application may expect older formats of Windows data, or it may expect user information to be in specific locations or formats. These types of problems apply primarily to applications written for Windows 95, Windows 98, or Windows Millennium Edition. Applications written exclusively for those platforms may use direct hardware access, which can greatly reduce operating system stability. Because of its Windows NT heritage, Windows XP SP1 requires that hardware access be handled through the correct channels.

To enable a better user experience, Microsoft has integrated technologies for application compatibility into Windows XP SP1. These technologies are applied whenever an application is installed on the operating system, whether in the course of a system upgrade or during regular operations. Some of these technologies work automatically to apply compatibility fixes, while others can be selected by users or administrators. This section addresses one available to users, the Program Compatibility Wizard. If users have an application compatibility problem they can use the wizard to make setting adjustments and run the application successfully.

Overview: Using the Program Compatibility Wizard in a managed environment

IT administrators who want to get an application to work quickly, without addressing compatibility for the application throughout the organization, may choose to use the Program Compatibility Wizard. You can use the wizard in situations where you want to determine quickly whether the prepackaged compatibility fixes can resolve problems you encounter, particularly if you are working on a computer where the Application Compatibility Toolkit is not installed. For more information about the Application Compatibility Toolkit, see Appendix D, "Application Compatibility Toolkit."

One of the most difficult tasks in network administration is monitoring and controlling which applications users install on their computers. When users try to install an incompatible application they may choose to run the Program Compatibility Wizard. In Windows XP SP1 users can access the Program Compatibility Wizard by default through All Programs\Accessories. The wizard asks users if they want to send files that contain "information about the settings you selected and whether the problems were fixed." Users can then choose to send this information to Microsoft. Allowing users to do this, however, may present a privacy problem for highly managed organizations.

Note As an alternative to running the Program Compatibility Wizard, users can set the compatibility properties for an application manually through the Compatibility tab of an executable file's Properties sheet. To do this you right-click the file name, click **Properties**, click **Compatibility**, and then change the compatibility settings for your application.

Administrators can use Group Policy to control where data collected by the Program Compatibility Wizard is sent. You can prevent data transfer to the Internet using Group Policy settings related to error reporting and have data from the wizard sent to a server on your intranet instead of to Microsoft. For more details on this procedure, see "Controlling Program Compatibility Wizard data to prevent the flow of information to the Internet" later in this section.

How the Program Compatibility Wizard communicates with sites on the Internet

Although you can control information sent by the Program Compatibility Wizard, it is designed to communicate over the Internet to expedite problem solving. This subsection lists details of the communication process:

- **Specific information sent or received**: The results of the Program Compatibility Wizard data, including settings and problems that were encountered with the application being installed, are sent to Microsoft. The user is not uniquely identified.
- **Default and recommended settings**: Use of the Program Compatibility Wizard is enabled by default. Recommended settings are discussed in the next subsection, "Controlling Program Compatibility Wizard data to prevent the flow of information to the Internet."
- **Triggers**: In the last dialog box of the wizard, users are asked if they want to send information to Microsoft. Data is not sent automatically.
- **User notification**: See Triggers.
- **Logging**: There is no information related to the Program Compatibility Wizard entered into the event log.
- **Encryption**: HTTPS is used to perform the data transfer to Microsoft.
- **Access**: The Microsoft product group has access to the raw data only.
- **Privacy policy**: The privacy policy is the same as that associated with Windows Error Reporting (WER) data. If the user chooses to send information they are provided with a link to the privacy policy.
- **Transmission protocol and port**: The transmission protocol used is HTTP and the port is HTTPS 443.
- **Ability to disable**: You cannot disable the Program Compatibility Wizard. Using Group Policy, you can prevent data from being sent to the Internet.

For more information on the type of information sent to Microsoft, how the data is used, encryption, and the privacy policy, see the section of this white paper titled "Windows Error Reporting."

Controlling Program Compatibility Wizard data to prevent the flow of information to the Internet

Using Group Policy you can configure the **Report Errors** policy setting to prevent data from the Program Compatibility Wizard from being sent to Microsoft. By using configuration options within error reporting you can have the data sent to a server on your intranet instead of to Microsoft. When you configure error reporting this way you activate Corporate Error Reporting (CER).

Use the following table to help you determine how you would configure error reporting to control how or whether data is sent to the Internet from the Program Compatibility Wizard.

Group Policy settings for configuring error reporting

Policy setting	What it does	Configuration options
Report Errors (enabled)	Errors are reported to Microsoft through the Internet or to a server on your intranet. Enabling **Report Errors** will override any settings made using Control Panel for error reporting. Default values will be used for any error reporting settings that are not configured, even if settings were previously adjusted through Control Panel.	Can select: • Do not display links to any Microsoft provided "more information" Web sites • Do not collect additional files • Do not collect additional computer data • Force queue mode for application errors Can enter: • Corporate file path • Replace instances of the word "Microsoft" with
Report Errors (disabled)	Users will not be given the option to report errors. If Display Error Notification is enabled, users will still get a message indicating that a problem has occurred, but they will not have the option to report it.	Not applicable
Report Errors (not configured)	Users will be able to adjust the setting using Control Panel, which is set to "enable reporting" by default on Windows XP.	Not applicable

For more information on configuration options and using Corporate Error Reporting, see the section of this white paper titled "Windows Error Reporting."

If you use this approach for reporting errors, the user experience with the Program Compatibility Wizard does not change. The dialog box that presents the option of sending data to Microsoft is the same. If the user selects Yes, the data is sent to the designated server on your intranet.

Procedure for controlling information sent to the Internet from the Program Compatibility Wizard

Use the following procedure to send error reports, including data from the Program Compatibility Wizard, to a server on your intranet instead of to Microsoft.

To send data from the Program Compatibility Wizard to a server on your intranet

1. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.
   For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for learning about Group Policy."

2. Click **Computer Configuration**, click **Administrative Templates**, click **System,** and then double-click **Error Reporting**.
3. In the details pane, double-click **Report Errors,** and then click **Enabled**.
4. In **Corporate upload file path**, enter a UNC (Universal Naming Convention) path (\\*servername**sharename*).

Note You can also configure various other elements of error reporting to suit the needs of your organization. You can review the error reports in the event log, or use the Corporate Error Reporting tool to filter reports described in the section of this white paper titled "Windows Error Reporting."

Remote Assistance

The following sections provide information about:

- The benefits of Remote Assistance
- How Remote Assistance communicates with sites on the Internet
- How to control Remote Assistance to prevent the flow of information to and from the Internet

Benefits and purposes of Remote Assistance

With Microsoft Windows XP Professional Service Pack 1 (SP1), a user or administrator can use Remote Assistance to get help from a member of the organization's support staff. Users or administrators can also collaborate in other ways through screen sharing. Remote Assistance is a convenient way for support professionals to connect to a computer from another computer running a compatible operating system, such as Windows XP, and to show the users or administrators a solution to their problem.

Using Windows Messenger Service or a MAPI-compliant e-mail program, such as Microsoft Outlook or Outlook Express, you can provide support to users by connecting to their computer. After you are connected you can view their computer screen, communicate with them in real time about what you both see on their computer, send files, use voice communication, and use your mouse and keyboard to work on their computer.

Overview: Using Remote Assistance in a managed environment

Through Help and Support Center users can access Remote Assistance by default and have someone inside or outside your network connect to their computer. In Help and Support Center users can click Invite a friend to connect to your computer with Remote Assistance, or click Tools\Remote Assistance.

While a firewall on your organization’s network will likely prevent outsiders from connecting directly to a computer on your intranet, the potential for users to connect remotely to someone either within your intranet or outside your network is available through Remote Assistance. As an administrator in a highly managed environment you might want to prevent users from using this feature. You can do this during your deployment of Windows XP SP1, or post-deployment using Group Policy.

In a domain environment there is also the option of a support person or IT administrator offering unsolicited assistance. From Help and Support Center using Tools\Offer Remote Assistance, an administrator in the domain may offer assistance to users in the same domain without being asked; however, users can decline the invitation. This capability should also be strictly controlled with Group Policy. Controlling the use of unsolicited as well as solicited Remote Assistance is described further in the subsection "Controlling Remote Assistance to prevent the flow of information to and from the Internet."

How Remote Assistance communicates with sites on the Internet

When a user (referred to as the "novice") initiates a request for assistance through either the e-mail option or the Save invitation as a file option in Remote Assistance, Windows XP starts Help and Support Center. Help and Support Center then passes the information to Remote Assistance. Remote Assistance then parses the file and starts the process of initiating a Remote Assistance session with the user’s computer that created the file.

When the person who is being contacted (the "expert") accepts the invitation from the novice, Remote Assistance calls Help and Support Center application programming interfaces (APIs) to initiate the session. Help and Support Center relies on Terminal Services to negotiate the session. Help and Support Center passes the Remote Assistance invitation (the "ticket") file to Terminal Services. The Remote Assistance session is established using RDP (Remote Desktop Protocol) and port 3389 through Terminal Services on the novice and expert computers.

There are safeguards built into the Remote Assistance feature. All sessions are encrypted and can be password-protected. The novice (user soliciting the assistance) sets the maximum time for the duration of the ticket. Also, firewalls on your organization's network might prevent users from making a connection. The following information presents additional details on how information transfer over the Internet takes place when a connection is made:

- **Specific information sent or received**: Information that is transmitted in a Remote Assistance ticket includes user name, IP address, and computer name. Information necessary to provide functionality for Remote Assistance (screen sharing, file transfer, voice) is sent in real time using point-to-point connections.
- **Default and recommended settings**: Anyone with access to Help and Support Center can access the Remote Assistance feature. Users can prevent someone from using Remote Assistance to take control of their computer by declining an invitation.
- **Triggers**: A user connects to another computer by first establishing contact with the expert by using an invitation through e-mail, instant messaging, or by saving an invitation as a file and transferring it manually, such as on a floppy disk, to the expert.
- **User notification**: The expert is asked through e-mail to provide help to the novice. A connection is not made unless the expert accepts the invitation. Or, in the case of unsolicited assistance, the novice has to click Yes to start a connection when an offer of assistance is received.
- **Logging**: Events such as a user initiating a connection or a user accepting or rejecting an invitation are recorded in the event logs.
- **Encryption**: The RDP (Remote Desktop Protocol) encryption algorithm and RTC (Real-Time Communication) encryption algorithm for voice are used. The RDP encryption algorithm is RC4 128-bit.
- **Access**: No information is stored at Microsoft.
- **Privacy policy**: There is no associated privacy policy.
- **Port and transmission protocol**: The port is 3389 and the transmission protocols are RDP and RTC.
- **Ability to disable**: Yes, using an unattended installation answer file and Group Policy, and locally through Control Panel.
- **Firewall protection**: Any firewall that blocks port 3389 should not allow a connection to users outside the firewall. This does not prevent users from within the firewall from connecting to each other.

For more information about the Remote Assistance connection process, see article 300692, "Description of the Remote Assistance Connection Process" in the Microsoft Knowledge Base at:

support.microsoft.com/default.aspx?scid=kb;en-us;300692

Controlling Remote Assistance to prevent the flow of information to and from the Internet

Administrators can control the use of Remote Assistance in the following ways:

- Answer files for unattended installation to block or control the use of Remote Assistance
- Group Policy to disable users or administrators from soliciting or offering Remote Assistance
- Local user controls of Remote Assistance through Control Panel

Answer file entries and Group Policy settings are described in detail in this subsection. Procedures for disabling Remote Assistance are presented in the next subsection.

Using unattended or remote installation

You can disable Remote Assistance, or control various aspects of it during workstation deployment by using standard methods for unattended or remote installation. The [PCHealth] section of an answer file is the section in which to place the entries for this feature. The following table describes those entries.

Answer file entries for controlling Remote Assistance

Entry	Description
RA_AllowFullControl	Specifies whether a person (other than the end user of the computer) can take full control of the computer from a separate location once the Remote Assistance session is established. When the entry is **RA_AllowFullControl = 0**, the person other than the end user can view the end user's desktop but cannot take control of the end user's computer.
RA_AllowToGetHelp	Specifies whether to enable Remote Assistance. When the entry is **RA_AllowToGetHelp = 0**, Remote Assistance is disabled.
RA_AllowUnsolicited	Specifies whether to enable unsolicited Remote Assistance. When the entry is **RA_AllowUnsolicited = 0**, unsolicited Remote Assistance is disabled.
RA_MaxTicketExpiry	Specifies the maximum time, in seconds, after which a Remote Assistance invitation expires.

As an example, the entry for disabling Remote Assistance is:

```
[PCHealth]
RA_AllowToGetHelp = 0
```

For more information about unattended installation, see Appendix A, "Resources for learning about automated installation and deployment."

Using Group Policy

There are two Group Policy settings you can configure to control the use of Remote Assistance:

- **Solicited Remote Assistance**

  Use this policy setting to determine whether or not solicited remote assistance is allowed from a computer. In **Solicited Remote Assistance** the user of a computer explicitly requests help from another party.

  Important When you disable this policy setting in Windows XP SP1, **Offer Remote Assistance** and unsolicited remote assistance are also disabled. This will be changed in a future release.

- **Offer Remote Assistance**

Use this policy setting to determine whether a support person or IT administrator (expert) can offer remote assistance to a computer without a user explicitly requesting it first through e-mail, a file, or instant messaging.

These policy settings are located in Computer Configuration\Administrative Templates\System\Remote Assistance. Configuration options for these policy settings are described in the following table.

Group Policy settings for controlling Remote Assistance

Policy setting	Description
Solicited Remote Assistance (enabled)	When this policy setting is enabled a user can request help and an expert can connect to the computer. Sending a help request does not explicitly give the expert permission to connect to the computer and to control it. When the expert tries to connect, the user will still be given a chance to accept or deny the connection (giving the expert view-only privileges to the user's desktop) and will afterward have to explicitly click a button to give the expert the ability to remotely control the desktop if remote control is enabled. Additional configuration options are available when you enable this policy setting.
Solicited Remote Assistance (disabled)	When this policy setting is disabled a user cannot send a request for assistance and an expert cannot connect to the computer in response to a user request.
Solicited Remote Assistance (not configured)	When this policy setting is not configured, the individual user will be able to configure solicited remote assistance through Control Panel. The default settings through Control Panel are: solicited remote assistance is enabled, buddy support is enabled, and remote control is enabled. The maximum ticket time is 30 days.
Offer Remote Assistance (enabled)	When this policy setting is enabled, you can offer remote assistance. When you configure this policy setting, you have two choices: you can select either "Allow helpers to only view the computer" or "Allow helpers to remotely control the computer." In addition to making this selection, when you configure this policy setting you also specify the list of users or user groups that will be allowed to offer remote assistance. Administrators can offer remote assistance by default; they do not need to be added to the list.
Offer Remote Assistance (disabled or not configured)	If you disable or do not configure this policy setting, users or groups cannot offer unsolicited remote assistance to this computer.

For additional configuration options see the Remote Assistance policy settings in the Group Policy Object Editor. To find more information about the Group Policy Object Editor, see Appendix B, "Resources for learning about Group Policy."

Procedures for disabling Remote Assistance

This section presents procedures administrators can use for disabling Remote Assistance.

To disable the use of Remote Assistance using Group Policy

1. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.

For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for learning about Group Policy."

2. Click **Computer Configuration**, click **Administrative Templates**, click **System**, and then click **Remote Assistance**.
3. In the details pane, double-click **Solicited Remote Assistance**.
4. In the Solicited Remote Assistance dialog box, select **Disabled**.
5. Click **Apply**, and then click **Next Setting**.
6. In the Offer Remote Assistance dialog box, select **Disabled**.

To disable the use of Remote Assistance through Control Panel

1. In Control Panel, double-click **System**.
2. Click the **Remote** tab.
3. Under Remote Assistance, clear the check box labeled **Allow Remote Assistance invitations to be sent from this computer**.

To disable the use of Remote Assistance by using an answer file (unattended installation)

1. Using the methods you prefer for unattended installation or remote installation, create an answer file. For more information about unattended and remote installation, see Appendix A, "Resources for learning about automated installation and deployment."
2. In the [PCHealth] section of the answer file, include the following entry:

   RA_AllowToGetHelp = 0

Search Companion

The following sections provide information about:

- The benefits of Search Companion
- How Search Companion communicates with sites on the Internet
- How to control Search Companion to prevent the flow of information to and from the Internet

Benefits and purposes of Search Companion

The Microsoft Search Companion Web service enables users to search for files and folders on their desktop computer, to search for files, people, and other computers on their internal network, and to search for information on the Internet. Search Companion uses Indexing Service to maintain an index of all the files on users' computers, making searches faster.

When employing Search Companion, users can specify several search criteria. For example, they can search for files and folders by name, type, or size. They can find files based on when they were last modified, or search for files containing specific text. When searching for information on the Internet, Search Companion allows users to enter search queries in natural language (meaning informal, or conversational language). It then suggests the best way to conduct the search, and sends the query to Internet services that are most likely to yield positive results.

Overview: Using Search Companion in a managed environment

When the user searches the Internet using Search Companion, the following information is collected:

- The text of the Internet search query
- Grammatical information about the query
- The list of tasks (suggestions) that the Search Companion Web service recommends to refine the search
- Any tasks the user selected from the recommendation list

Search Companion does not collect:

- Personal information
- Demographic information

Microsoft does not use the information it collects to identify the user individually and does not use such information in conjunction with other data sources that may contain personal data. Microsoft does not collect information when the user searches on the local system, LAN, or intranet.

The Search Companion Web service is designed to upgrade automatically as new features become available. It therefore uses the Internet connection periodically to check for and replace necessary files.

If you want to disable the Search Companion Web service, you can do so by changing to Classic Search for the Internet. Microsoft Windows does not collect any query information when Classic Search is used. You can also disable Search Companion by modifying the registry settings. The procedures for both of these methods are described later in this section of the white paper.

How Search Companion communicates with sites on the Internet

Search Companion in Microsoft Windows XP Professional Service Pack 1 (SP1) improves the search process by consolidating search tasks, optimizing searches for the most common scenarios, and offering suggestions for refining the search.

The form the user creates to collect search criteria will post information to an ASP page that displays the search results. The search pages use a combination of XML and Microsoft Visual Basic® development system, Scripting Edition (VBScript) and Microsoft JScript® development software for accessing the search objects. Because the script is run on the server, users can view the search pages from any browser.

Search Companion uses XML files to define both UI and some functional parameters of its tasks (for example, what list of file extensions comprises the "Music" category of files). The first time in each Search Companion session that an XML file is referenced, Search Companion checks to see if a later version of that XML file is available from sa.windows.com. The "check" is really a file download request, conditioned on the modified date of the file. If there is a later version of the XML file, Search Companion downloads it and replaces the earlier version. The XML files are located in a language-specific subfolder of \Windows\srchasst\, and if the current user does not have administrative credentials, the old XML file cannot be overwritten.

This section describes various aspects of the data that is sent to and from the Internet through Search Companion, and how the exchange of information takes place:

- **Specific information sent or received**: When you search the Internet using Search Companion, the following information is collected regarding your use of the service: the text of your Internet search query, grammatical information about the query, the list of tasks which the Search Companion Web service recommends, and any tasks you select from the recommendation list.
- **Default and recommended settings**: Search Companion is enabled by default.
- **Triggers**: The user selects Start\Search\Search the Internet\
- **User notification**: There is no provision in Search Companion for user review or notification of data sent, but users can opt out by disabling Search Companion entirely.
- **Uniquely identify users**: The user is not uniquely identified. Session-based cookies are used to maintain state information, but these randomly assigned GUIDs do not persist across browser sessions.
- **Logging**: No information is collected when you search your local system, LAN, or intranet. The only "storage" is the Internet Information Services (IIS) log of the file request. Search Companion does not record your choice of Internet search engines, and it does not collect or request any personal or demographic information.
- **Encryption**: There is no encryption of data.
- **Access**: No user information is collected. The IIS logs are cycled annually, that is, logs are retained for twelve months, and discarded in the thirteenth month following collection.
- **Privacy policy**: The privacy policy is located at the following Web site:

  sa.windows.com/privacy/
- **Transmission protocol and port**: The transmission protocol is HTTP and the port is 80.
- **Ability to disable**: The feature can be disabled by changing to Classic Search.

Controlling Search Companion to prevent the flow of information to and from the Internet

You can disable the Search Companion Web service by changing preferences to Classic Search for the Internet. You can also disable Search Companion by changing the registry settings manually. Procedures for both of these approaches are provided in the following subsection.

Procedures for configuration of Search Companion

Search Companion can be configured in several ways as described previously. This section lists the procedures to change or disable the features in accordance with your company’s security policies.

To change to Classic Search for the Internet

1. Click **Start**, and then click **Search**.
2. Click **Change preferences**.
3. Click **Change Internet search behavior**.
4. Click **With classic Internet search**.

To disable Search Companion through the registry key

1. Start the Registry Editor (Regedt32.exe).
2. Locate the following key in the registry:
   HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CabinetState
3. Set the value of **Use Search Asst** to "No."

Windows Error Reporting

The following sections provide information about:

- The benefits of Windows Error Reporting
- How Windows Error Reporting communicates with sites on the Internet
- How to control Windows Error Reporting to prevent the flow of information to and from the Internet

Benefits and purposes of Windows Error Reporting

The Windows Error Reporting feature in Windows XP Professional Service Pack 1 (SP1) provides a service which allows Microsoft to track and address errors relating to the operating system, Windows components, and applications. This service, called the Error Reporting service, gives users the opportunity to send data about errors to Microsoft and to receive information about them. Moreover, it is an essential problem-solving tool allowing developers to address customer problems in a timely manner and to improve the quality of Microsoft products.

In addition to having users send information to Microsoft, in some cases Microsoft may provide information to users, such as a way to work around a problem or a link to a Web site for updated drivers, patches, or Microsoft Knowledge Base articles.

Overview: Using Windows Error Reporting in a managed environment

In Windows XP SP1, error reporting is enabled by default and users can report system and application errors to Microsoft if they choose to. When an error occurs, a dialog box is displayed allowing the user to report the problem. When a user chooses to report the problem, technical information about the problem is collected and then sent to Microsoft over the Internet. No information is sent unless the user confirms that the error report be sent to Microsoft.

Users can configure or disable error reporting through the Control Panel\System\Advanced tab. They can configure error reporting to send specified information such as system errors only, or errors for Windows components, such as Windows Explorer, Paint, or Microsoft Internet Explorer; and for applications, such as Microsoft Word.

Since error reporting is a valuable service it is not recommended that IT administrators disable it, but that they control what information is reported and where it is sent. For an organization where privacy is a concern, it is recommended that the IT department review and filter error reports before they are sent to Microsoft.

The best method to use to prevent the automatic flow of error reporting information to and from the Internet is to redirect error reports to a server on your intranet using Group Policy and to set up Corporate Error Reporting (CER). You can configure error reporting to control various aspects of how errors are reported. While it is not recommended, you can also completely disable error reporting on client computers.

IT administrators can use the Corporate Error Reporting tool to manage error reports that have been redirected to a network server. You use the tool to review the redirected error reports and then filter the reports that are sent to Microsoft based on your policies and the data contained within the error report. The tool is also useful for determining the types of problems users are experiencing most often.

If you have not yet deployed Windows XP SP1, you can use unattended installation files to configure error reporting in the same way as in Group Policy. If it is necessary in your organization to completely disable Windows Error Reporting you can do so with the unattended installation file or with Group Policy. For more information about these methods, see "Controlling error reporting to prevent the flow of information to and from the Internet" later in this section.

How Windows Error Reporting communicates with sites on the Internet

The data that Microsoft collects is used strictly for the purpose of tracking down and solving problems that users are experiencing. The information is stored in a secure database with limited access. This subsection describes various aspects of the data that is sent to and from the Internet during error reporting, and how the exchange of information takes place.

- **Specific information sent or received**: For Windows XP SP1, Microsoft collects various types of information related to two types of errors, user mode or application errors, and kernel mode or operating system failures. Some information that uniquely identifies the user might inadvertently be collected as part of the crash report. This information, if present, is never used to contact a user. The specific data collected is described later in this subsection. Also, Microsoft may send information about a problem, including links to Web sites.
- **Default and recommended settings**: Error reporting for application and system errors is enabled by default on clients running Windows XP SP1. For more information about recommended settings, see "Controlling Windows Error Reporting to prevent the flow of information to and from the Internet" later in this section.
- **Triggers**: The opportunity to send an error report is triggered by application or system errors.
- **User notification**: A dialog box appears notifying users that an error has occurred and asks if they want to send an error report to Microsoft. Users can review the data that will be sent.
- **Logging**: Descriptions of system and application errors are recorded in the event log.
- **Encryption**: All data that could include personally identifiable information is encrypted (HTTPS) during transmission. The "crash signature," which includes such information as the application name and version, module name and version, and offset (location) is not encrypted.
- **Access**: Microsoft employees and contingent staff who have submitted a business justification for reviewing the information are granted access to the data.
- **Privacy policy**: The privacy policy for Microsoft Error Reporting is located at the following Web site:

  watson.microsoft.com/dw/1033/dcp.asp

  Details of this policy are presented in "Types of data collected" later in this section.
- **Transmission protocol and port**: The transmission protocol is HTTP Put and Request and the ports are HTTP 80 and HTTPS 443.
- **Ability to disable**: The feature can be disabled through Group Policy or by users on their own computer.

Types of errors reported

In Windows XP SP1 there are two types of errors that are reported, user mode and kernel mode.

User mode reporting

When a user mode error occurs, such as an application error, the Error Reporting service does the following:

- Displays an alert stating that Windows XP detected a problem.

  Users can choose to report the problem or not. If they do report it, they will see that the information is being sent to Microsoft.

- Sends a problem report to Microsoft.

  Users may then be queried for additional computer information and again may choose to send it or not. If they choose to do so, the Error Reporting service sends the error report to Microsoft. Users might be prompted to provide additional information to complete the error report. When the process is complete, users have the option of selecting More Information, which directs them to updated drivers, patches, or Microsoft Knowledge Base articles.

If the error report indicates that one or more non-Microsoft products were involved in causing the problem, Microsoft may send the report to the respective companies. Qualified software or hardware developers (employed by Microsoft or one of its partners) will analyze the fault data and try to identify and correct the problem.

Kernel mode reporting

When a kernel mode or system error occurs, Windows XP SP1 displays a Stop message and writes diagnostic information to a memory dump file. When users restart their computer by using normal mode or safe mode (with networking) and log on to Windows XP, the Error Reporting service gathers information about the problem and displays a dialog box that gives them the option of sending a report to Microsoft.

Types of data collected

The Error Reporting service collects Internet Protocol (IP) addresses, which are not used to identify users. It does not intentionally collect anyone’s name, address, e-mail address, computer name, or any other form of personally identifiable information. It is possible that such information may be captured in memory or in the data collected from open files, but Microsoft does not use it to identify users.

In rare cases, such as problems that are especially difficult to solve, Microsoft may request additional data, including sections of memory (which may include memory shared by any or all applications running at the time the problem occurred), some registry settings, and one or more files from the user’s computer. The user’s current documents may also be included. When additional data is requested, the user can review the data and choose to send the information or not.

In Windows XP SP1 the specific type of data that is collected when application errors or kernel failures occur is as follows.

Application errors

If you have an application error the Error Reporting service collects the following information:

- The Digital Product ID, which can be used to identify your license.

- Information regarding the condition of the computer and the application at the time when the error occurred. This includes data stored in memory and stacks, information about files in the application's directory, as well as the operating system version and the computer hardware in use. This information is packaged into what is called a "minidump." The minidump contains the following:
  - Exception information: This is information regarding the problem that occurred; it tells Microsoft what kind of instruction the application received that caused it to generate an error.
  - System information: This is data about the kind of CPU (processor) you have and what operating system you are running.
  - A list of all the modules that are currently loaded and their version information.
  - A list of all the threads that are currently running. For each thread, the current context and the whole stack are collected.
  - Global data.

  The minidump data is shown as a hexadecimal representation that the user cannot read.

  Note For the exact specification of the minidump format, see the Microsoft Platform SDK, which is available on the Microsoft Developers Network (MSDN) Web site.

Windows kernel failures

Windows kernel fault reports contain information about what your operating system was doing when the problem occurred. These event reports contain the minimum information that can help to identify why the operating system stopped unexpectedly. The report includes:

- The operating system name (for example, Microsoft Windows XP).
- The operating system version (for example, 5.1.24260.0).
- The operating system language as represented by the locale identifier (LCID) (for example, 1033 for United States English). This is a standard international numeric abbreviation.
- The loaded and recently unloaded drivers. This identifies the modules used by the kernel when the Stop error occurred, and the modules that were used recently.
- The list of drivers in the Drivers folder on your hard disk; for example, C:\Winnt\System32\Drivers for Windows 2000.
- The file size, date created, version, manufacturer, and full product name for each driver.
- The number of available processors.
- The amount of random access memory (RAM).
- The time stamp that indicates when the Stop error occurred.
- The messages and parameters that describe the Stop error.
- The processor context for the process that stopped. This includes the processor, hardware state, performance counters, multiprocessor packet information, deferred procedure call information, and interrupts (requests from software or devices for processor attention).
- The process information and kernel context for the halted process. This includes the offset (location) of the directory table and the database that maintains the information about every physical page (block of memory) in the operating system.

- The process information and kernel context for the thread that stopped. This information identifies registers (data-storage blocks of memory in the processor) and interrupt request levels, and includes pointers to data structures for operating system data.
- The kernel-mode call stack for the interrupted thread. This is a data structure that consists of a series of memory locations and includes a pointer to the initial location.

Controlling error reporting to prevent the flow of information to and from the Internet

To prevent the automatic flow of information to and from the Internet when users report errors, you can configure error reporting in two ways: while deploying Windows XP SP1 using answer files with unattended or remote installation, or after deployment using Group Policy. There may be some aspects of error reporting you want to configure using answer files, and others you may want to configure using Group Policy. Review the tables in this subsection to determine the configuration options that will work best for your organization.

Using unattended installation

You can configure error reporting by using standard methods for unattended or remote installation. The **[PCHealth]** section of an answer file is the section in which to place the entries for this feature. The following table describes those entries.

Entries for configuring error reporting in an answer file (for unattended installation)

Entry	Description
ER_Display_UI	Specifies whether Setup notifies the user that an error has occurred and shows details about the error. When the entry is **ER_Display_UI = 0**, Setup does not notify the user that an error has occurred.

ER_Enable_Applications
ER_Include_EXE(*n*)
and
ER_Exclude_EXE(*n*)
	ER_Enable_Applications = All
	Reports errors for all applications except for those listed in ER_Exclude_EXE(*n*).
	ER_Enable_Applications = Listed
	Reports errors only for those applications listed in ER_Include_EXE(*n*). You can automatically include Microsoft applications by using ER_Include_MSApps.
	ER_Enable_Applications = None
	Reports no application errors.
	Examples of entries that list included applications are:
	ER_Include_EXE1 = iexplore.exe
	ER_Include_EXE2 = explorer.exe
	Examples of entries that list excluded applications are:
	ER_Exclude_EXE1 = calc.exe
	ER_Exclude_EXE2 = notepad.exe

ER_Enable_Kernel Errors	Specifies whether Windows reports errors in the Windows kernel. When the entry is **ER_Enable_Kernel Errors = 0**, Windows does not report errors in the Windows kernel.
ER_Enable_Reporting	Specifies whether Windows automatically reports errors. When the entry is **ER_Enable_Reporting = 0**, Windows does not report errors.
ER_Enable_Windows_ Components	Specifies whether to report errors in Windows components. When the entry is **ER_Enable_Windows_Components = 0**, Windows does not report errors in Windows components. To exclude individual Windows components, use

	ER_Exclude_EXE(*n*), as described earlier in this table.
ER_Force_Queue_Mode	Specifies whether to send all reports in queue mode. When the entry is **ER_Force_Queue_Mode = 0**, Windows does not send reports in queue mode.
ER_Include_MSApps	Specifies whether to track and report errors in Microsoft applications. When the entry is **ER_Include_MSApps = 0**, errors in Microsoft applications are not tracked and reported.
ER_Include_Shutdown_ Errs	Specifies whether to report shutdown errors. When the entry is **ER_Include_Shutdown_Errs = 0**, shutdown errors are not reported.

For complete details about the entries for error reporting, see the resources listed in Appendix A, "Resources for learning about automated installation and deployment." Be sure to review the information in the Deploy.chm file (whose location is provided in that appendix).

Using Group Policy

To enable Corporate Error Reporting it is recommended you perform these steps:

- Configure the **Error Reporting** policy settings in Group Policy so that error reports go to a server on your intranet.
- Use the Corporate Error Reporting tool to filter reports.

It is recommended you enable error reporting through Group Policy because then you can override actions users may take, and you can redirect error reports to a server on your intranet instead of to the Internet. Once you have initiated Corporate Error Reporting, you can use this tool to manage error reports.

In addition to the **Error Reporting** policy settings, this subsection also includes a list of the **Advanced Error Reporting** policy settings you may want to use for additional configuration options.

Using Error Reporting policy settings

To configure clients for Corporate Error Reporting you need first to enable the **Report Errors** policy setting. Once you enable this policy setting, you can enter a file path to a server on your intranet, limit data that is exchanged on the Internet when errors are reported, control how users interact with the Error Reporting service, and take other steps to control information.

For details about locating the error reporting policy settings, see "Procedures for configuring error reporting" later in this section. The following table describes the settings.

Group Policy settings for configuring error reporting

Policy setting	What it does	Configuration options
Report Errors (enabled)	Errors are reported to Microsoft through the Internet or to a server on your intranet. Enabling **Report Errors** will override any settings made using Control Panel for error reporting. Default values will be used for any error reporting settings that are not configured, even if settings were adjusted through Control Panel.	Can select: • Do not display links to any Microsoft provided "more information" Web sites • Do not collect additional files • Do not collect additional computer data • Force queue mode for

		application errors Can enter: • Corporate file path • Replace instances of the word "Microsoft" with
Report Errors (disabled)	Users will not be given the option to report errors. If **Display Error Notification** is enabled, users will still get a message indicating that a problem occurred, but they will not have the option to report it. Disabling Report Errors is useful for servers that do not have interactive users.	Not applicable
Report Errors (not configured)	Users will be able to adjust the setting using Control Panel, which is set to "enable reporting" by default on Windows XP.	Not applicable
Display Error Notification (enabled)	This setting controls whether or not a user is given the choice to report an error. When enabled, the user will be notified that an error has occurred and will be given access to details about the error.	Not applicable
Display Error Notification (disabled)	The user is not given the choice of whether to report the error. If **Report Errors** is enabled, the error will be automatically reported, but the user will not be notified that an error has occurred. Disabling this setting is useful for servers that do not have interactive users. (Default setting for servers.)	Not applicable
Display Error Notification (not configured)	The user will be able to adjust the setting through Control Panel, which is set to enable notification by default.	Not applicable

To find more information about the Group Policy Object Editor, see Appendix B, "Resources for learning about Group Policy."

Using Advanced Error Reporting policy settings

When you enable error reporting you can choose to specify the types of errors that are reported. In a highly managed environment administrators might want to do this based on the kinds of information included in the error report (see "Types of data collected" in the previous subsection). Whether or not you use this option might depend on whether you allow users, or have administrators, send error reports to Microsoft.

For details about locating the error reporting settings, see "Procedures for configuring error reporting" later in this section. With **Advanced Error Reporting** you can configure the following policy settings:

- **Default application reporting settings**
- **List of applications to always report errors for**
- **List of applications to never report errors for**
- **Report operating system errors**
- **Report unplanned shutdown events**

When you configure these policy settings they will override any adjustments to error reporting users might make through Control Panel.

To find more information about the Group Policy Object Editor, see Appendix B, "Resources for learning about Group Policy."

How controlling error reporting can affect users

What users will see on their computer when an error occurs depends on how you have configured the **Error Reporting** policy settings. Depending on which policy settings you have enabled and which options you have configured, you can have users input varying amounts of information during error reporting, or none at all. You can choose not to have any user interface when a fault occurs, or, you can have a user notified that an error has occurred, but not allow for the opportunity to send a report.

Another factor in how the user interface is affected is how you have configured the following policy settings: **List of applications to always report errors for** and **List of applications to never report errors for**. For more information about these policy settings, see "Procedures for configuring error reporting" and "Related Links" later in this section.

The following table presents two examples of what the user will see when an error occurs if you have enabled the **Error Reporting** policy settings and if you have entered a path to a server. The first option presents the recommended policy settings.

How sending error reports to an intranet server affects the user interface

Configuration options	User interface
Report Errors enabled; **Corporate file path** entered; **Display Error Notification** enabled	• User is notified that an error occurred • User might be asked for additional data • Reports go to an intranet server
Report Errors enabled; **Corporate file path** entered; **Display Error Notification** not enabled	• No user interface • Reports automatically go to an intranet server

Procedures for configuring error reporting

This section presents the recommended procedure for enabling Corporate Error Reporting by configuring the **Report Errors** policy setting in Group Policy, for administrators who want to control the information that goes out to the Internet. This section also outlines a procedure for locating Group Policy settings for error reporting and a procedure for configuring error reporting during unattended installation of Windows XP SP1 by using an answer file.

Use the following procedure to configure the **Report Errors** policy setting so error reports are sent to a server on your intranet instead of to Microsoft.

To enable Corporate Error Reporting

1. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.

For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for learning about Group Policy."

2. Click **Computer Configuration**, click **Administrative Templates**, click **System**, and then double-click **Error Reporting**.
3. In the details pane, double-click **Display Error Notification**, and then select **Enabled**.
4. Click **Next Setting**.
5. Double-click **Report Errors**, and then select **Enabled**.
6. In the Corporate upload file path box, enter a UNC (Universal Naming Convention) path (\\servername\sharename).

   Note Administrators can then filter the error reports using the CER tool described in the previous subsection, "Controlling error reporting to prevent the flow of information to and from the Internet."

Use the following procedure to locate the Group Policy settings described in "Using Group Policy" earlier in this section.

To locate Group Policy settings for error reporting

1. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.
   For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for learning about Group Policy."
2. Click **Computer Configuration**, click **Administrative Templates**, click **System**, and then click **Error Reporting**.
3. View the Group Policy settings that are available. For more information about these settings, see the table in "Using Error Reporting policy settings" earlier in this section.
4. Click **Advanced Error Reporting settings**.
5. View the advanced settings that are available. For more information about these settings, see the list in "Using Advanced Error Reporting policy settings" earlier in this section.

To configure error reporting during unattended installation by using an answer file

1. Using the methods you prefer for unattended installation or remote installation, create an answer file. For information about unattended installation, and for complete details about the entries for error reporting, see the resources listed in Appendix A, "Resources for learning about automated installation and deployment." Be sure to review the information in the Deploy.chm file (whose location is provided in that appendix).
2. In the [PCHealth] section of the answer file, create entries according to the table in "Using unattended installation" earlier in this section.

Related Links

For more information about Windows Error Reporting see:

msdn.microsoft.com/library/default.asp?url=/library/en-us/debug/base/windows_error_reporting.asp

Using Windows XP Professional with Service Pack 1 in a Managed Environment

To obtain the Corporate Error Reporting tool see:

oca.microsoft.com/en/cerintro.asp

To read the Microsoft privacy policy for error reporting see:

watson.microsoft.com/dw/1033/dcp.asp

Windows Media Player

The following sections provide information about:

- The benefits of Windows Media® Player
- How Windows Media Player communicates with sites on the Internet
- How to control Windows Media Player to limit the flow of information to and from the Internet

Note This section describes the version of Windows Media Player included with Windows XP Professional SP1. Other versions of Windows Media Player might differ from the version described in this section. For more information, see the Windows Media Player Web site at:

www.microsoft.com/Windows/WindowsMedia/

Benefits and purposes of Windows Media Player

Microsoft Windows Media Player (also called the Player) enables users to play and organize digital media files on their computer and on the Internet. Users can play CDs and DVDs (if they have DVD hardware), create custom CDs, listen to radio stations, search for and organize digital media files, and copy files to a portable device.

Windows Media Player for Microsoft Windows XP Professional Service Pack 1 (SP1) enables you as the administrator to configure the Player to control access to certain consumer features. The management and deployment features enable you to bring customized media functionality to your organization's employees to enhance productivity.

For more information about deploying and managing Windows Media Player in an enterprise environment, see the Windows Media Web site at:

www.microsoft.com/Windows/WindowsMedia/

Overview: Using Windows Media Player in a managed environment

Windows Media Player is an integral component of Windows XP and is installed at the time you install the operating system. Windows Media Player is not an optional Windows component and cannot be uninstalled. You can, however, use an answer file to hide entry points to the user interface. You can also customize the Player to make certain aspects of it either available, of limited use, or unavailable to the user in accordance with policies in your organization. This section of the white paper describes how Windows Media Player communicates with the Internet and how to control the flow of information to and from the Internet. It gives procedures for using Group Policy to control the user interface, playback, and networking as well as procedures for using registry keys to control the Player updates. The following table summarizes the solutions for various security requirements.

Security options for Windows Media Player

Security level	Solution
Highest security, least flexibility.	Windows Media Player entry points hidden. For more

	information about hiding the entry points during unattended installation, see "Procedures for configuration of Windows Media Player" later in this section.
High security but requires investment in time and money to implement an internal Windows Media server.	Windows Media Player available but with access only to the organization's intranet media server. For more information, see the Help on a server running Windows 2000, specifically, the Help that is installed when you install the Windows Media Services component.
Good security; user access to Internet limited. Requires knowledge of which external sites are trustworthy.	Inclusion list (through the firewall or proxy or both) that contains only those Internet sites that are approved for access by clients.
Good security, but access to Internet only available to users who need it most. Implies that training is provided to selected users who are held accountable.	Only certain users have access to the Internet. All others are restricted by various means.
Good security. Flexible but requires investment of money and training for firewall or proxy server implementation.	Fine-tuned settings on firewall, proxy server, or both.
Moderate security, moderate flexibility.	Use Group Policy settings (on a server) to configure Windows Media Player on clients. For more information, see "Controlling Windows Media Player to limit the flow of information to and from the Internet" and "Procedures for configuration of Windows Media Player" later in this section.
Lowest security, but most flexible.	Free access for all.

How Windows Media Player communicates with sites on the Internet

Windows Media Player opens locally on the desktop when the user navigates through the Start menu or clicks a shortcut. By default, Windows Media Player opens www.WindowsMedia.com automatically through either a LAN or a modem connection. When the connection is made, WindowsMedia.com provides the following nine key features:

- Metadata retrieval
- Metadata submission
- Media guide
- Radio tuner
- Codec download
- Player update
- Newsletter signup
- Downloadable skins
- Downloadable visualizations

To support the playback of secure content, Windows Media Player will also contact:

- Non-Microsoft digital rights management (DRM) license servers
- Microsoft DRM upgrade service

The other common Internet connections that Windows Media Player makes are to Windows Media servers run by content providers.

The following list describes various aspects of the data that is sent to and from the Internet through Windows Media Player, and how the exchange of information takes place:

- **Specific information sent or received**: The key features of WindowsMedia.com listed previously communicate information between the Internet and the user’s computer as follows:
    - **Non-Microsoft digital rights management (DRM) license servers.** The license servers enable users to acquire licenses to play back content protected with Microsoft's DRM technology. The license acquisition process updates the user's DRM revocation and exclusion lists. These lists are used to block compromised applications from accessing secure content.
    - **Microsoft DRM upgrade service.** The upgrade service provides users with the option to upgrade their DRM components should the secure content they want to play require upgraded components (for example, an individualized black box).
    - **Windows Media servers run by content providers.** To provide streaming media, it is necessary for Windows Media Player to communicate directly with a media server. These servers are typically operated by non-Microsoft content providers, and are not under Microsoft's control.
    - **Metadata retrieval.** The requested metadata, including album art, track names, lyrics, and even artist bios, is returned and stored in the user's media library for offline use. A CD table of contents or DVD identification is sent.
    - **Metadata submission.** A service that enables users to submit corrections to the WindowsMedia.com metadata database. A cookie (if not blocked), CD table of contents or DVD identification, and user's corrected metadata are sent.
    - **Media guide.** Media Guide is a set of Web pages focused on streaming media, hosted within the Windows Media Player interface. A cookie is sent up (if not blocked); the Media Guide Web page from WindowsMedia.com is returned.
    - **Radio tuner.** Radio Tuner is a set of Web pages focused on Internet radio stations, hosted with the Windows Media Player interface. A cookie is sent up (if not blocked); the Radio Tuner Web page is returned, with pre-sets (if the cookie is not blocked).
    - **Codec download.** A service that enables users to acquire certain codecs during playback if they are not resident on the user's system. A cookie (if not blocked) and codec are sent up; a codec is returned and installed if available. (A codec, short for compressor/decompressor, is software that compresses or uncompresses audio or video data.)
    - **Player update.** A service that enables users to detect and acquire updated Windows Media Player components. A cookie (if not blocked) and a version number of Windows Media Player components are sent; components are returned and installed if available and the user has consented. The automatic check and manual update options are only available to users with administrative credentials.
    - **Newsletter signup.** The Media Guide provides a link to the MSN newsletter service to enable users to sign up for the WindowsMedia.com newsletter. An MSN cookie (if not blocked) and the user's e-mail address are sent directly to the MSN newsletter service.
    - **Downloadable skins.** Additional Skins is a Web page containing extra downloadable skins, hosted in the Windows Media Player interface. A cookie is sent up (if not blocked); the Downloadable Skins Web page is returned.

  - **Downloadable visualizations.** Additional Visualizations is a Web page containing extra downloadable visualizations, hosted in the Windows Media Player interface. A cookie is sent up (if not blocked); the Downloadable Visualizations Web page is returned.
  - **Media library.** The Media Library lists the user's collection of audio and video files, as well as links to sources for audio and video. This information can be accessed by other software on the user's computer and on the Internet.
  - **Cookies**. Windows Media Player uses the Internet as a networking and information source. When accessing the Internet, cookies may be downloaded to the user's computer or uploaded to a media service.
  - **Site logs**. There are two types of logs created as follows:
    - **Raw IIS log**. A standard Internet Information Services (IIS) log that records all requests to the server. This log includes the IP address of the client and a cookie. It is not encrypted.
    - **Tracking log**. This log contains all requests. It includes the IP address of the client and a cookie. It is neither encrypted nor correlated with personally identifiable information.
- **Default and recommended settings**: All of the Windows Media Player features are enabled by default. Not all options, however, such as the GUID that uniquely identifies the player, are enabled by default. Recommended settings are described in the next subsection, "Controlling Windows Media Player to limit the flow of information to and from the Internet."
- **User notification and triggers**: The WindowsMedia.com features are triggered individually by various user interactions as listed below. The user may or may not be notified at that time depending on the feature being triggered.
  - **Metadata retrieval.**
    - **Notification.** The user is not notified.
    - **Trigger.** When the user first inserts a CD or DVD, or when the user requests detailed information, (for example, by using the Media Details button), information is retrieved automatically from WindowsMedia.com.
  - **Metadata submission.**
    - **Notification**. The user is notified.
    - **Trigger.** When the user submits corrected metadata in the CD Wizard, information is sent to WindowsMedia.com.
  - **Media guide.**
    - **Notification.** The user is not notified.
    - **Trigger.** The media guide is triggered automatically if the Player option is set to start in media guide mode or when the user selects Media Guide from the menu.
  - **Radio tuner.**
    - **Notification**. The user is not notified.
    - **Trigger.** When the user selects Radio Tuner from the menu the radio station selection screen is triggered.
  - **Codec download.**
    - **Notification.** There is no Windows Media Player pop-up message.
    - **Trigger.** A security dialog box will pop up if the site is not trusted. The Windows Media Player status bar will indicate that a codec is being downloaded.

    - **Player update.**
        - **Notifications.** The user is notified. The user is prompted to download but can decline to do so.
        - **Trigger.** At a set frequency, if the user is online and is logged on as an administrator, a check is made for updated Windows Media Player components.
    - **Newsletter signup.**
        - **Notification.** The user is notified, although the user does not have to subscribe to the newsletter.
        - **Trigger.** The trigger occurs when the user selects "subscribe to our free newsletter" on the Media Guide.
    - **Downloadable skins.**
        - **Notification.** The user sees the download progress dialog box after the selection is made.
        - **Trigger.** The user selects "more skins" from the Skin Chooser menu, which brings up the Downloadable skins Web site. When the user selects a skin from this screen the skin is downloaded.
    - **Downloadable visualizations.**
        - **Notification.** The user sees the download progress dialog box after the selection is made.
        - **Trigger.** The user selects "Download Visualizations" from the Tools\Download Visualizations menu, which brings up the Downloadable visualization Web site. When the user selects a visualization from this screen the visualization is downloaded.
    - **Media library.**
        - **Notification.** The user is not notified.
        - **Trigger.** The trigger occurs when adding purchased media to the library from WindowsMedia.com or another media vendor. Access can be turned off through the Media Library tab on the Tools\Options menu.
    - **Cookies.**
        - **Notification.** The user is not notified.
        - **Trigger.** The trigger occurs automatically when a Web site is accessed. Cookie downloads can be blocked from the Privacy tab in Internet Options.
- **Logging**: Logging occurs when information is sent from the Player to a streaming media server. Logging informs the server of various pieces of information so that services can be improved. The information includes such details as connection time and the Internet protocol (IP) address of the computer that is connected to the server (typically a Network Address Translation [NAT] or proxy server). It also includes the version, identification number (ID), date, and protocol of Windows Media Player. Most information is neither unique nor traceable to the user's computer. For more detailed information about the exchange of information in Windows Media Player, read the privacy statement located on the Windows Media Player's Help menu.
- **Encryption**: Windows audio media can be encrypted using the Secure Audio Path feature in Digital Rights Management (DRM). The Secure Audio Path feature maintains audio encryption beyond the Player application. It is a feature of Microsoft Windows that maintains the security and protection of digital music that has been encrypted by using DRM technology. Secure Audio Path provides an infrastructure for maintaining copy protection on music. The client can progressively download content from a Web server using HTTPS. A client and server may also use Internet Protocol security (IPSec) to encrypt packets that traverse the network.

- **Privacy policy**: Microsoft Windows Media Player and WindowsMedia.com both have published privacy statements that detail their data collection and use practices. These documents are available to users at the following locations:
  - The Windows Media Player privacy statement at:

    www.microsoft.com/windows/windowsmedia/software/v8/privacy.asp
  - The WindowsMedia.com privacy statement at:

    windowsmedia.com/privacy/privacystatement.asp
- **Transmission protocol**: With Windows Media Player you can specify that selected protocols are used while receiving streaming media from a Microsoft Media Server (MMS) URL as follows:

  Note Protocol selection is only effective when MMS rollover is involved. When the SDK tries to open an MMS URL, it automatically selects the best protocol to receive the data, that is, if the existing firewall configuration is specified. The first time the software development kit (SDK) opens an MMS URL, it tries to connect to the server by using the MMS protocol over User Datagram Protocol (UDP). If this fails, it tries to use MMS over Transmission Control Protocol (TCP). If this also fails, it makes a final attempt by using HTTP. This process is called "protocol rollover."

  - **Multicast**. Routers will not pass multicast streams across an intranet.
  - **UDP**. UDP is used with port selection if required due to firewall or proxy issues. If the UDP check box is selected and the UDP ports box is blank, the Player uses default ports when playing content from an MMS URL. If the UDP check box is not selected, the information in the UDP ports box is ignored. If using a NAT, UDP because will fail and should therefore be disabled.
  - **TCP**
  - **HTTP**. When the HTTP protocol is selected, the HTTP protocol is used to receive streaming media from an MMS URL. Streaming media from an MMS URL that requires the UDP or TCP protocols cannot be played.

  If none of the protocols is selected, content from an MMS URL cannot be played.
- **Port**: The Windows Media Player client communicates across random ports as designated by the operating system. The server port is a "well-known port" as follows:
  - **Transmission protocol and port**: The transmission protocol is HTTP and the port is 80.
  - **Microsoft Media Server (MMS) UDP or TCP**: The port number is 1755.

  In a TCP connection there is only one socket created. You therefore need only one port number on the client and one on the server. Commands (such as play, pause, and fast forward) and data (audio and video) are sent across the same socket connection. In UDP connections, however, the client makes a TCP connection to the server and sends commands over it. The server then opens a UDP socket to the client. It is over this second socket that the audio and video data is sent. And it is this second socket that firewalls and proxies typically block.

  If the enterprise network implements a firewall that prevents users from receiving streams that use the UDP or TCP protocols, Windows Media Player can be configured to work with firewalls as described in the following list items.
- **Windows Media and firewalls:** Windows Media normally streams through UDP/IP on a wide range of ports (these port numbers are provided later in this list). Microsoft is aware of the possible security issues that a range of this size can cause, so Microsoft has also enabled Windows Media to stream with TCP/IP through a single port (1755). For those sites where opening a port that is not "well-known" is a problem, Windows Media can also stream through HTTP on port 80. HTTP streaming from Windows Media Services is disabled by default. Windows Media Technologies was formerly known as

NetShow Player; some firewalls have a preconfigured NetShow Player setting, which may work for Windows Media.

- **Firewall settings for Windows Media**
  There are five primary scenarios to consider when you set up a firewall to accommodate Windows Media:

  - Using Windows Media Player behind a firewall to access content outside the firewall
  - Using Windows Media Player outside a firewall to access content on a Windows Media server behind a firewall
  - Using Windows Media Encoder outside a firewall to communicate with a Windows Media server behind the firewall, or to communicate between two servers across a firewall
  - Using Windows Media Administrator outside a firewall to manage a Windows Media server behind a firewall
  - IP multicast

  This section of the white paper describes only the first and last scenarios, that is, the client behind the firewall scenario and the IP multicast scenario. In the examples below, the in port is the port that the server uses to get past the firewall. The out port is the port that Microsoft Windows Media Player or other clients use to communicate with the server. The port assignment is random between 1024 and 5000.

  - **Client configuration behind a firewall**
    A firewall configuration that enables users with Windows Media Player behind a firewall to access Windows Media servers outside the firewall is:

    Streaming ASF with UDP
    Out: TCP on 1755
    Out: UDP on 1755
    In: UDP between ports 1024 and 5000 (As a security measure, estimate the number of ports you will need by determining how many clients you expect and open only that number of ports.)

    Streaming ASF with TCP
    In and out: TCP on port 1755

    Streaming ASF with HTTP
    In and out: TCP on port 80

  - **IP multicast**
    Choosing to allow Windows Media streaming through IP multicast is simply a choice to allow traffic that is addressed to the standard Class D IP addresses (224.0.0.0 through 239.255.255.255). As of this writing, most routers have IP multicast disabled; router companies made a decision to have their equipment default to disable IP multicast at a time when a typical video stream took up 30 percent of a 10BaseT network. (10BaseT is the Ethernet standard for baseband local area networks using twisted-pair cable carrying 10 Mbps in a star topology network.)

    Microsoft is working with major router vendors to reverse this situation, now that media streams are compressed and standards are in place that eliminate unwanted multicast traffic. The Internet Group Management Protocol (IGMP) supported by Windows Media assures that multicast traffic passes through the network only when a client has requested it. Windows Media streams are highly compressed, usually only taking up the bandwidth of a single modem connection.

    The following firewall configuration enables IP multicasting:

Streaming ASF with multicast
IP multicast address range: 224.0.0.1 through 239.255.255.255
To enable IP multicasting you must allow packets sent to this standard IP multicast address range to come through the firewall. This IP multicast address range must be enabled on both client and server sides, as well as on every router in between.

- **Ability to disable**: All key features are enabled by default; however, each can be disabled either directly through the Tools\Options menu in Windows Media Player or through changes to the registry settings. The procedures for disabling the key features are described later in this section. You can also disable access to Windows Media Player through Group Policy or an answer file during unattended installation. For more information, see "Settings that can be controlled through Group Policy" and "Procedures for configuration of Windows Media Player" later in this section.
- **Uniquely identify user**: Windows Media Player at no time requests any personally identifiable information (such as name, address, or phone number).

Controlling Windows Media Player to limit the flow of information to and from the Internet

The most secure method of controlling information to and from the Internet is to eliminate access to Windows Media Player entry points during unattended installation. Individual Windows Media Player features can, however, be controlled in two ways, either through the Tools\Options menu on the user interface or through the use of Group Policy. The recommended method for controlling the features in a managed environment is through Group Policy, with an additional change to the registry that will prevent the Player update. The following lists describe options that can be controlled through the Windows Media Player user interface, through Group Policy, and through other means. For more details about configuring these options, see "Procedures for configuration of Windows Media Player" later in this section.

Settings that can be controlled through the user interface in Windows Media Player

You can control the following through the user interface in Windows Media Player:

- **Metadata retrieval.** Do not insert the CD or DVD, or in Windows Media Player, work offline.
- **Metadata submission.** Do not submit metadata.
- **Media guide.** Clear the **Start Player in Media Guide** check box.
- **Radio tuner.** Use a custom skin with no Radio Tuner access.
- **Codec download.** Clear or check the **Download Codecs Automatically** check box.
- **Newsletter signup.** Use a custom skin; eliminating access to Media Guide eliminates access to the newsletter signup.
- **Downloadable skins.** Use a custom skin that does not display downloadable skins.
- **Downloadable visualizations.** Use a custom skin that does not display downloadable visualizations.

Settings that can be controlled through Group Policy

The following settings for Windows Media Player can be controlled through Group Policy. For a procedure for locating the Group Policy settings for configuring Windows Media Player, see "Procedures for configuration of Windows Media Player" later in this section.

- User Interface settings
  - **Set and Lock Skin**

    You can use a custom skin that eliminates access to functionality you want to control, specifically, Radio Tuner, Media Guide, display of downloadable skins, or display of downloadable visualizations.
  - **Do Not Show Anchor**
- Playback setting
  - **Prevent Codec Download**
- Networking settings
  - **Hide Network Tab**

    When you hide this tab, users cannot configure network settings for Windows Media Player.
  - **Streaming Media Protocols**

    The protocols to choose from are Multicast, UDP (enter UDP ports if required), TCP, and HTTP, as described in "How Windows Media Player communicates with sites on the Internet" earlier in this section.
  - **Configure HTTP Proxy**

    This Group Policy setting is ignored if the setting for **Streaming Media Protocols** is enabled and HTTP is not selected. When this Group Policy setting is disabled, the Player cannot use the HTTP proxy and the user cannot change the HTTP proxy settings on the Network tab in Windows Media Player.
  - **Configure MMS Proxy**

    This Group Policy setting is ignored if the setting for **Streaming Media Protocols** is enabled and multicast is not selected. When this policy setting is disabled, the MMS proxy cannot be used and the user cannot change the MMS proxy settings on the Network tab in Windows Media Player.
  - **Configure Network Buffering**

Other ways to control Windows Media Player

You can control several aspects of Windows Media Player through means other than the user interface or the individual Group Policy settings for Windows Media Player. You can:

- Prevent users from starting Windows Media Player through Group Policy by adding wmplayer.exe to a list of Windows applications that cannot be run. For more information, see "To prevent users from starting Windows Media Player by using Group Policy" later in this section.
- Use the firewall or proxy or both to block access to the WindowsMedia.com Web site.
- Use a registry key, "DisableAutoUpdate," to disable the automatic update feature in Windows Media Player. For more information, see "Disabling the update feature in Windows Media Player for Windows XP using a registry key" later in this section.

Procedures for configuration of Windows Media Player

Windows Media Player can be configured in several ways as described previously. This subsection provides procedures for:

- Locating Group Policy settings for configuring Windows Media Player
- Preventing users from starting Windows Media Player by using Group Policy
- Accessing the Network tab on the user interface in Windows Media Player (to set streaming media protocols)
- Using a registry key to disable the automatic update feature in Windows Media Player
- Removing visible entry points to Windows Media Player during unattended installation by using an answer file

Important To prevent users from manually updating Windows Media Player, the recommendation is to ensure that those users are not set up with administrative credentials on their computers.

To locate Group Policy settings for configuring Windows Media Player

1. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.
   For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for learning about Group Policy."
2. Click **User Configuration**, click **Administrative Templates**, click **Windows Components**, and then click **Windows Media Player**.
3. View the Group Policy settings that are available. For more information about these settings, see the list under "Settings that can be controlled through Group Policy" earlier in this section.

To prevent users from starting Windows Media Player by using Group Policy

1. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.
   For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for learning about Group Policy."
2. Click **User Configuration**, click **Administrative Templates**, and then click **System**.
3. In the details pane, double-click **Don't run specified Windows applications**.
4. Select **Enabled**, click **Show**, click **Add**, and then enter the application executable name, wmplayer.exe.

Setting streaming media protocols

There are two methods for setting streaming media protocols. One method, described in the following procedure, is to use the Network tab to both configure the protocols and proxy settings that you want Windows Media Player to use when receiving streaming media files, and to then hide the Network tab through the use of Group Policy in Windows Media Player. The second method is to use Group Policy directly. For more information about using Group Policy, see "To locate Group Policy settings for configuring Windows Media Player" and "Settings that can be controlled through Group Policy" earlier in this section.

To access the Network tab on the user interface in Windows Media Player

1. On the **Tools** menu, click **Options**, and then click **Network**.
2. The following options are listed on the **Network** tab:

- **Protocols.** Specifies the protocols Windows Media Player can use to receive a stream. Select one or more of the following:
  - Multicast
  - UDP
  - TCP
  - HTTP

  By default, all protocols are selected, which means that the Player attempts to use each protocol to receive a stream. Because the Player can receive files using a variety of protocols, it is recommended that you select all protocols.
- **Use ports.** Specifies a particular port, or port range, if UDP is the protocol used to receive streaming content. This option is useful if your network or firewall administrator has established a specific port that enables streaming content to pass through. Unless otherwise instructed, Windows Media streams attempt to pass through firewalls on port 1755.
- **Proxy settings**. Select one of the following:
  - HTTP
  - MMS

  Proxy settings specify how each protocol operates with a proxy server. Proxy servers are used when networks are protected by firewalls. If your network is behind a firewall, and you do not know how to configure your settings, please refer to the "Windows Media and Firewalls" item in the list under "How Windows Media Player communicates with sites on the Internet," or consult your network administrator.
- **Configure** button**.** Click this button to change the proxy settings of the selected protocol. The following table lists the options for configuring a protocol to work with a proxy server.

Options for configuring a protocol to work with a proxy server

This option	Specifies that
Autodetect proxy settings	The Player discovers the ports that are open and uses them to receive streaming content.
Use proxy settings of the Web browser	The Player uses the same HTTP configuration as your browser to access network communication.
Do not use a proxy server	The Player does not attempt to communicate with a proxy server. Typically, this means that the Player does not receive streaming content from the Internet.
Use the following proxy server	The Player uses the proxy server and port you specify. Select Bypass proxy server for local addresses if you do not want the Player to use the proxy server when streams are from local servers.

Disabling the update feature in Windows Media Player for Windows XP using a registry key

Windows Media Player for Windows XP does not have a Group Policy setting to disable the check for update features. There is another option that can be used to disable the automatic update feature although the administrative option outlined above is recommended. This option is to use a registry key to disable the automatic update feature. Manually setting a registry policy key means, however, that the Group Policy architecture is not notified. The instructions for setting this key are described below.

To set the registry key

1. Start the Registry Editor (Regedt32.exe).
2. Locate the following key in the registry: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft
3. On the Edit menu, click **Add Key**, and then add the following key name: **WindowsMediaPlayer**
4. After you add the **WindowsMediaPlayer** key, select the **WindowsMediaPlayer** key.
5. On the Edit menu, click **Add Value**, and then add the following registry value:
   - Value Name: DisableAutoUpdate
   - Data Type: REG_DWORD
   - Radix: Decimal
   - Value: 1
6. Quit the Registry Editor.

Windows Media Player also has the ability to update codecs from the Internet regardless of whether the Player updates were disabled.

To remove visible entry points to Windows Media Player during unattended installation by using an answer file

1. Using the methods you prefer for unattended installation or remote installation, create an answer file. For more information about unattended and remote installation, see Appendix A, "Resources for learning about automated installation and deployment."
2. In the [Components] section of the answer file, include the following entry:

   WMPOCM = Off

   Note This entry does not remove any Windows code, including any Windows Media Player code, other than these visible entry points.

Windows Messenger

The following sections provide information about:

- The benefits of Windows Messenger
- How Windows Messenger communicates with sites on the Internet
- How to control Windows Messenger to limit or prevent the flow of information to and from the Internet

Benefits and purposes of Windows Messenger

Windows Messenger enables users to communicate instantly and to collaborate with their selected contacts. Windows Messenger version 4.7 in Microsoft Windows XP Professional Service Pack 1 (SP1) is the real-time communication (RTC) feature for Windows XP and offers not only instant messaging, but also voice and video communications, application sharing, whiteboard, file transfer, and remote assistance.

Overview: Using Windows Messenger in a managed environment

In an Internet environment, Windows Messenger utilizes the Passport infrastructure for directory and authentication services. In a managed environment, access to the Internet for these services may not be available or desirable, so this infrastructure is provided by the Exchange 2000 Instant Messaging service, a component of Exchange 2000 Server. For more information about Exchange 2000 Instant Messaging service see the Microsoft Web site at:

www.microsoft.com/exchange/techinfo/administration/2000/ClientKeys.asp

How Windows Messenger communicates with sites on the Internet

Windows Messenger clients initiate communication between one another through a server component that provides for client registration, configuration, and presence (the online status of a user’s contacts). This server component may also act as a broker in client-to-client communication, such as when instant messaging is used. There is currently a server solution for Internet-based communication (Microsoft .NET Messenger Service) and a server solution for enterprise instant messaging (Microsoft Exchange 2000 Instant Messaging Server).

Windows Messenger users can register with a variety of servers or services and subscribe to their contacts' online status. Windows Messenger provides these capabilities by supporting a number of different protocols, which are listed later in this subsection under "Transmission protocol."

Main services supported by Windows Messenger

Windows Messenger provides three network service providers for the following services:

- **.NET Messenger Service**: This service enables anyone with a Microsoft .NET Passport account to communicate using the Internet. The user must have a .NET Passport account to use Windows Messenger.

- **Exchange 2000 Instant Messaging service**: Exchange 2000 Instant Messaging service is a component of Exchange 2000 Server that uses Microsoft Active Directory directory service to provide additional security and identity controls critical to enterprise customers. The Exchange 2000 Instant Messaging service uses the same MSN or Windows Messenger client interface as the Microsoft .NET Messenger Service. With the Windows Messenger client update for Exchange 2000 Instant Messaging service, however, you are able to simultaneously connect to both the .NET Messenger Service and your organization's Exchange 2000 Instant Messaging service.
- **IETF SIP proxy services**: This is a communications service account that provides instant messaging within an organization or network. The communications service is built using Session Initiation Protocol (SIP) services-based messaging and presence extensions, available on Windows and other servers operating SIP services.

Windows Messenger can work with multiple server types and protocols concurrently. This might be appropriate in an environment where the Exchange 2000 Instant Messaging service is used for internal communication and the .NET Messenger Service for external communication.

The rest of this subsection describes various aspects of the data that is sent to and from the Internet through Windows Messenger and how the exchange of information takes place.

- **Specific information sent or received**: When users sign up for the .NET Messenger Service, Microsoft requests their Passport member name, phone numbers (optional), the list of contacts with whom they can send and receive instant messages, and reciprocal information about those contacts. Some user options, such as their privacy settings, are stored so that those settings are available when they sign in from a different computer or device. Certain information about your computer hardware and software is automatically collected by the .NET Messenger Service. This information may include your IP address, browser type, and operating system. This information is used by Microsoft for the operation of the service, to maintain quality of the service, and to provide general statistics regarding use of the .NET Messenger Service.

  Windows Messenger also sends less obvious information:

  - Change in presence status
  - Typing indicator traffic during a conversation
  - Network Address Translation (NAT) traversal traffic to echo the server for the PC to Phone feature
  - Universal Plug and Play NAT traversal traffic
- **Default and recommended settings**: The default is set to enable open communication between internal and external networks. Because the information sent and received is not secure, however, it is recommended that access to external networks such as the Internet be restricted.
- **Triggers**: Windows Messenger is triggered when the user double-clicks the icon in the task bar and opens the Windows Messenger window. The user then has access to all of the tools and actions offered.
- **User notification**: The traffic is part of Windows Messenger and the user is not notified when information is sent or received.
- **Logging**: No logging takes place on the client.
- **Encryption**: There is no encryption of information with Windows Messenger, with the exception of passwords. Any information is sent in plaintext format and is therefore open to viewing by anyone.
- **Access**: Computer-to-computer communication using the .NET Messenger Service sends and receives data in plaintext over the Internet. Instant messaging conversations are relayed through a server in the service. Sending and receiving data in plaintext over the Internet means that no encryption or similar security feature is protecting that communication.

- **Privacy policy**: Microsoft Windows Messenger has a published privacy statement that details the practices for data collection and use. This document is available to users at:

  messenger.microsoft.com/support/privacypolicy.asp

  The privacy policy can also be found on the Windows Messenger user interface in the Help menu.

- **Port**:

  - **Audio and video**. When negotiating an audio-video (AV) session, dynamic ports are chosen for the audio-video stream. Dynamic ports are used to enable the application to work regardless of which other applications are running on the system and using port resources. The actual Real-time Transport Protocol (RTP) streams are sent using dynamically allocated User Datagram Protocol (UDP) ports in the range of 5004 through 65535. Without a way to open these UDP ports on any firewall in the path dynamically, the streams will fail to reach their destination.

  - **Application sharing and whiteboard**. Since a specific port is used for the Transmission Control Protocol (TCP) data connection (1503), if the client is behind a NAT device, the port must be mapped to that client.

  - **Instant messaging**. To enable your network users to have a direct connection to instant messaging services, you need to:

    - Open outgoing TCP connections to port 1863 on your proxy servers.

    - Let your network users know which kind of proxy server your network uses (HTTP, SOCKS4, or SOCKS5) and provide them with the corresponding details (including server name and port number) so they can enter that information about the Connection tab of the Options dialog box (under Tools\Options).

    - Make sure the internal local area network has access to the Domain Name System (DNS) servers to resolve the names of external hosts such as messenger.msn.com.

  - **File transfer**:

    - Both incoming and outgoing TCP connections use this range of ports: 6891 through 6900. This allows up to 10 simultaneous file transfers per sender. If you open only port 6891, users will be able to do only one file transfer at a time.

    - The TCP ports need to be configured so that sockets on a port remain open for extended periods of time.

    - File transfer may not work if you are behind a NAT device.

- **Transmission protocol**:

  - **Presence**. Presence in Windows Messenger tells users about the online status of the people on their contacts lists. When a user logs on to Windows Messenger, an attempt is made to log on to each configured network. Although each of these networks is different and may use different protocols, the result of the attempted logon is that the user's presence is registered on each network. Part of this process involves establishing a relationship with a Presence and Rendezvous service.

  - **.NET Messenger Service and Exchange 2000 Instant Messenging service**. This is a TCP connection, but the protocols used over that TCP connection to provide presence are different. This connection is used for server-mediated communications—including forwarding messages from instant messaging. If a SIP server solution is used, the relationship is established through SIP Register, Subscribe, and Notify methods, usually using UDP as a transport.

  - **Instant messaging**. Instant messaging is a mode of communication and collaboration in Windows Messenger. The protocol used for initialization and communication on the instant messaging session depends on the server or service being used. For .NET Messenger Service or Exchange 2000 Instant Messenging service, the instant messaging text is carried over a TCP connection. When a SIP proxy server is used for instant messaging, the server can be configured to transfer the text over TCP/UDP or HTTPS.

  - **Voice and video**. Voice and video calls, another mode of communication and collaboration in Windows Messenger, require more than a server-mediated session. A peer-to-peer session is needed to avoid creating congestion on the server. In this case, the servers and services are used to initiate the session setup and media type negotiation using SIP and SDP. The Real-time Transport Protocol (RTP) is used over UDP for the actual voice or video streams.
  - **Application sharing and whiteboard**. Application sharing and whiteboard, modes of communication and collaboration in Windows Messenger, start out the same as a voice or video session. The Rendezvous service is used to exchange the initial invitations, followed by a SIP invitation and acknowledgment in which the session information is exchanged. The differences between AV and application sharing and whiteboard are:
    - The actual media exchange is done using T.120 over a TCP connection as opposed to UDP. (T.120 is a set of International Telecommunications Union specifications for multipoint data communications services within computer applications.) This connection may be initiated by the one being called, as are many Windows Messenger calls.
    - The port used for the TCP connection is set at port 1503 on the called station.
  - **File transfer**. File transfer is a mode of communication and collaboration in Windows Messenger. A file transfer session, used when the client requests to send a file to a peer, is initiated similarly to AV and application sharing and whiteboard—without the SIP invitation and acceptance exchange. Once the session is configured through the server, file transfer is accomplished using a TCP connection between the peers over a fixed range of ports.
  - **Remote assistance**. Remote assistance is a mode of communication and collaboration in Windows Messenger that uses Remote Desktop Protocol (RDP)—the same protocol used by Microsoft Terminal Services. RDP is built on top of a TCP connection. Windows Messenger sets up the remote assistance session using the server-based session invitation logic; this is similar to file transfer. The additional SIP invitation signaling is only added if a voice session is added in support of remote assistance.
- **Ability to disable**: Windows Messenger can be disabled through Group Policy. The procedures for this method are provided later in this section.

Controlling Windows Messenger to limit or prevent the flow of information to and from the Internet

Windows Messenger can be controlled in two ways, through the use of Group Policy in Windows 2000 Server at deployment time or through the use of registry keys. The recommended method for a managed environment is through the use of Group Policy. The procedures for both of these methods are given in the next subsection.

There are a number of configurations in which all the capabilities of Windows Messenger work seamlessly. There are also configurations where certain capabilities are limited or do not work. To resolve some of these issues, Windows Messenger uses the Universal Plug and Play infrastructure in Windows XP and earlier versions of the Windows operating system. This type of resolution will become more available as more Internet gateway devices add support for Universal Plug and Play.

In many networks, all of these features can be used without any changes to the network infrastructure. Certain networks, such as business or residential, may also deploy firewalls and NAT components. Some Windows Messenger features, mainly instant voice and video communications, experience reduced functionality when used in certain Internet scenarios. Windows Messenger features that are affected by NAT and firewall issues are:

- Instant messaging and presence
- Audio and video
- Application sharing and whiteboard
- File transfer
- Remote assistance

When Universal Plug and Play-enabled firewalls or NAT components are used between communicating parties, all of the new Windows Messenger features work as intended. There are network setups that require special configuring, however, for all of the new Windows Messenger features to work.

For more information on working with firewalls and NAT devices for Windows Messenger, see the white paper on the Microsoft Web site at:

www.microsoft.com/windowsxp/pro/techinfo/deployment/natfw/default.asp

Procedures for Windows Messenger

Windows Messenger can be configured in several ways as described previously in this section of the white paper. This subsection describes the procedures for changing or disabling the various features in accordance with your organization’s security policies.

The following sections provide information about:

- Preventing Windows Messenger from running on a computer running Windows XP
- Controlling policy in Windows Messenger using registry keys
- Removing visible entry points to Windows Messenger during unattended installation of Windows XP SP1 by using an answer file
- Enabling MSN Messenger traffic through an Internet Security and Acceleration (ISA) Server

How to prevent Windows Messenger from running on a computer running Windows XP

To prevent Windows Messenger from running by using Group Policy

1. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.
   For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for learning about Group Policy."
2. Click **Computer Configuration**, click **Administrative Templates**, click **Windows Components**, and then click **Windows Messenger**.
3. In the details pane, double-click **Do not allow Windows Messenger to run**, and then click **Enabled**.

Controlling policy in Windows Messenger using registry keys

In Windows Messenger version 4.7, policy control is done statically on the client using registry keys, as opposed to dynamically downloading the policies from a service. By setting policy control values in the registry, you can enforce different policies on the Windows Messenger client.

To control policy in Windows Messenger using registry keys

1. Start Registry Editor (Regedit.exe).
2. Locate and click the following registry key:
   HKEY_LOCAL_MACHINE\Software\Policies\Microsoft
3. On the Edit menu, point to **New**, click **Key**, and then type **Messenger** for the name of the new registry key.
4. Locate and click the following registry key:
   HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Messenger
5. On the **Edit** menu, point to **New**, click **Key**, and then type **Client** for the name of the new registry key.
6. Locate and click the following registry key:
   HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Messenger\Client
7. On the **Edit** menu, point to **New**, click **DWORD Value**, and then type **PreventRun** for the name of the new DWORD value.
8. Right-click the PreventRun value that you created, click **Modify**, and type **1** in the **Value data** box.
9. Quit Registry Editor.

Note This method also prevents applications that use the Windows Messenger application programming interfaces (APIs) from using Windows Messenger. Outlook 2002, Outlook Express 6, and the Remote Assistance feature in Windows XP are examples of programs that use these APIs and that depend on Windows Messenger.

To remove visible entry points to Windows Messenger during unattended installation by using an answer file

1. Using the methods you prefer for unattended installation or remote installation, create an answer file. For more information about unattended and remote installation, see Appendix A, "Resources for learning about automated installation and deployment."
2. In the [Components] section of the answer file, include the following entry:

   WMAccess = Off

Note This entry does not remove any Windows code, including any Windows Messenger code, other than these visible entry points.

How to enable MSN Messenger traffic through an ISA Server

Support for MSN Messenger is built into Microsoft ISA Server 2000 as a predefined protocol; however, if you enable packet filtering, MSN Messenger does not work without the following additional configuration:

To configure MSN Messenger for sending messages

1. Right-click **Protocol Rule**, and then click **New Rule**.

2. Type **Instant Messenger Rule** for the name of the rule, and then click **Next**.
3. Click **Allow**, and then click **Next**.
4. In the drop-down menu, click **Selected Protocols**, click **MSN Messenger** in the dialog box that opens, and then click **Next**.
5. Click **Next**.
6. Click **Any Request** on the **Client type** dialog box, and then click **Finish**.

To configure the packet filter

The type of packet filters to configure depends on the type of access you want to allow with MSN Messenger. First configure the packet filter to allow for simple MSN Messenger communication:

1. Right-click **Packet Filters**, and then click **New Filter**.
2. Type **Instant Messenger Outbound**, and then click **Next**.
3. Click **All ISA Server Computers in the array**, and then click **Next**.
4. Click **Allow packet transmission**, and then click **Next**.
5. Click **Custom** on the **Filter type** dialog box, and then click **Next**.
6. In the **IP Protocol** drop-down list, click **TCP**.
7. Under **Direction**, click **Both**.
8. Under **Local Port**, click **Dynamic**, change **Remote Port** to **Fixed Port**, and then for the Port Number type **1863**.
9. Click **Default IP addresses for each external interface on the ISA Servers computer**, and then click **Next**.
10. Click **All remote computers**, click **Next**, and then click **Finish**.

Windows Time service

The following sections provide information about:

- The benefits of the Windows Time service
- How the Windows Time service communicates with sites on the Internet
- How to control the Windows Time service to limit the flow of information to and from the Internet
- How to monitor and troubleshoot the Windows Time service after configuration is complete

Benefits and purposes of the Windows Time service

Many components of Microsoft Windows XP Professional Service Pack 1 (SP1) rely on accurate and synchronized time to function correctly. For example, without clocks that are synchronized to the correct time on all computers, Windows XP authentication might falsely interpret logon requests as intrusion attempts and consequently deny access to users.

With time synchronization, you can correlate events on different computers in an enterprise. With synchronized clocks on all of your computers, you ensure that you can correctly analyze events that happen in sequence on multiple computers. The Windows Time service automatically synchronizes a local computer’s time with other computers on a network to improve security and performance in your organization.

Overview: Using the Windows Time service in a managed environment

Computers keep the time on their internal clocks, which allows them to perform any function that requires the date or time. For scheduling purposes, however, the clocks must be set to the correct date and time, and they must be synchronized with the other clocks in the network. Without some other method in place, these clocks must be set manually.

With time synchronization, computers set their clocks automatically to match another computer's clock. One computer maintains very accurate time, and then all other computers set their clocks to match that computer. In this way, you can set accurate time on all computers.

The Windows Time service is installed by default on all computers running Windows 2000 and Windows XP. The Windows Time service uses Coordinated Universal Time (UTC), which is based on an atomic time scale and is therefore independent of time zone. Time zone information is stored in the computer's registry and is added to the system time just before it is displayed to the user.

The Windows Time service starts automatically on computers that are joined to a domain. (For computers that are not joined to a domain, you can start the time service manually.) In a domain, time synchronization takes place when the Windows Time service turns on during system startup. The Net Logon service looks for a domain controller that can authenticate and synchronize time with the client. When a domain controller is found, the client sends a request for time and waits for a reply from the domain controller. This communication is an exchange of Simple Network Time Protocol (SNTP) packets intended to calculate the time offset and roundtrip delay between the two computers.

How the Windows Time service communicates with sites on the Internet

In Windows XP, the Windows Time service automatically synchronizes the local computer's time with other computers on the network. The time source for this synchronization varies, depending on whether the computer is joined to a domain in the Active Directory directory service or to a workgroup.

When a computer running Windows XP is part of a workgroup

In this scenario, the default setting for the time synchronization frequency is set to "once per week," and this default setting uses the time.windows.com site as the trusted time synchronization source. This setting will remain until you manually set it otherwise. One or more computers might be identified as a locally reliable time source by configuring the Windows Time service on those computers to use a known accurate time source, either by using special hardware or a time source available on the Internet. All other workgroup computers can be configured manually to synchronize their time with these local time sources.

When a computer running Windows XP is a member of a domain

In this scenario, the Windows Time service configures itself automatically, using the Windows Time service that is available on the domain controllers.

The Windows Time service on a domain controller can be configured as either a reliable or an unreliable time source. The Windows Time service running on a client will attempt to synchronize its time source with servers that are indicated as reliable. The Windows Time service can configure a domain controller within its domain as a reliable time source, and it synchronizes itself periodically with this source. These settings can be modified or overwritten, depending on specific needs.

When a computer running Windows XP or Windows 2000 is not a member of a domain

The Windows Time service must be manually started for computers running Windows 2000 that are not members of a domain. For Windows XP computers that are not members of a domain, the Windows Time service is configured by default to synchronize its time source with time.windows.com. The Windows Time service starts automatically for computers running Windows XP. Computers running Windows XP use the Network Time Protocol (NTP), while computers running Windows 2000 use the Simple Network Time Protocol (SNTP).

The following list describes various aspects of the Windows Time service data that is sent to and from the Internet and how the exchange of information takes place:

- **Specific information sent or received**: The service sends information in the form of a network packet.
- **Default and recommended settings**: Computers that are members of an Active Directory domain synchronize time with domain controllers by default. Domain controllers synchronize time with their parent domain controller. By default, the root parent domain controller will not synchronize to a time source. The root parent domain controller can be set to either synchronize to a known and trusted Internet-based time source, or a hardware time device that provides an NTP or SNTP interface.
- **Triggers**: The Windows Time service is started when the computer starts. Additionally, the service will continue to synchronize time with the designated network time source and adjust the computer time of the local computer when necessary.

- **User notification**: Notification is not sent to the user.
- **Logging**: Information related to the service is stored in the Windows System event log. The time and network address of the time synchronization source is contained in the Windows event log entries. Additionally, warning or error condition information related to the service is stored in the Windows System event log.
- **Encryption**: Encryption is used in the network time synchronization for domain peers.
- **Port**: NTP and SNTP defaults to using User Datagram Protocol (UDP) port 123. If this port is not open to the Internet, you cannot synchronize your server to Internet SNTP servers.
- **Communication protocol**: The service on Windows 2000 implements SNTP to communicate with other computers on the network. The service on Windows XP implements NTP to communicate with other computers on the network.
- **Ability to disable**: Disabling the service has no direct effect on applications or other services. Applications and services that depend on time synchronization, such as Kerberos V5 authentication protocol, may fail, or they may yield undesirable results if there is a significant time discrepancy among computers.
- **Information storage**: The service does not store information, as all information that results from the time synchronization process is lost when the time synchronization service request is completed.

Controlling the Windows Time service to limit the flow of information to and from the Internet

Group Policy can be used to control the Windows Time service for computers that are running Windows XP SP1 to limit the flow of information to and from the Internet. Group Policy for computers running Windows 2000 does not include support for the Windows Time service. You can, however, import the Group Policy settings for Windows XP to Active Directory for a server running Windows 2000 and then access the policy settings through Group Policy to achieve the same configurations. For more information about importing Group Policy Administrative Templates, see Appendix C, "Importing Group Policy settings for Windows XP to a server running Windows 2000 SP3."

The synchronization type and NTP time server information can be managed and controlled through Group Policy. The Windows Time service Group Policy object (GPO) contains configuration settings that specify the synchronization type. When the synchronization type is set to Nt5DS, the Windows Time service synchronizes its time resource with the network domain controller. Alternatively, setting the type attribute to NTP configures the Windows Time service to synchronize with a specified NTP time server. The NTP server is specified by either its Domain Name System (DNS) name or its IP address when you select NTP as the synchronization type. For more general information about the Windows Time service, see "The Windows Time Service" on the Microsoft Web site at:

www.microsoft.com/windows2000/techinfo/howitworks/security/wintimeserv.asp

Clients on a managed network can be configured to synchronize computer clock settings to an NTP server on the network to minimize traffic out to the Internet and to ensure that the clients synchronize to a single reliable time source. If you choose to do so, you can disable time synchronization for both non-domain and domain computers running Windows XP by using Group Policy. The procedures for configuring the Windows Time service are given at the end of this section of the white paper.

How the Windows Time service can affect users and applications

Windows components and services depend on time synchronization. For example, the Kerberos V5 authentication protocol (supported on Windows 2000) on a Windows 2000 domain has a default time synchronization threshold of five minutes. Computers that are more than five minutes out of synchronization on the domain will fail to authenticate using the Kerberos protocol. This time value is also configurable, allowing for smaller thresholds. Failure to authenticate using the Kerberos protocol can prevent logons, access to Web sites, file shares, printers, and other resources or services within a domain.

When the local clock offset has been determined, the following adjustments are made to the time:

- If the local clock time of the client is behind the current time received from the server, the Windows Time service will change the local clock time immediately.
- If the local clock time of the client is more than three minutes ahead of the time on the server, the service will change the local clock time immediately.
- If the local clock time of the client is less than three minutes ahead of the time on the server, the service will quarter or halve the clock frequency for long enough to synchronize the clocks.
- If the client is less than 15 seconds ahead, it will halve the frequency; otherwise, it will quarter the frequency. The amount of time the clock spends running at an unusual frequency depends on the size of the offset that is being corrected.

Configuration settings for the Windows Time service

You can set the global configuration settings for the Windows Time Service by using Group Policy. For details about locating the Windows Time service policy settings, see "Procedures for configuring the Windows Time service" later in this section. The following table describes the settings.

Group Policy settings for configuring the Windows Time service

Policy setting	Effect of policy setting	Default setting
FrequencyCorrectRate	One over the rate at which the clock is corrected. If this value is too small, the clock will be unstable and will overcorrect. If the value is too large, the clock will take a long time to synchronize.	4
HoldPeriod	The period of time for which spike detection is disabled in order to bring the local clock into synchronization quickly. A spike is a time sample indicating that time is off a number of seconds, usually received after good time samples have been returned consistently.	5
LargePhaseOffset	A time offset greater than or equal to this value is considered suspicious by the time service. This occurrence might be caused by a noise spike.	1,280,000
MaxAllowedPhaseOffset	The maximum offset (in seconds) for which Windows Time service attempts to adjust the computer clock by using the clock rate. When the offset exceeds this rate, the service sets the computer clock directly.	300
MaxNegPhaseCorrection	The largest negative time correction in seconds that the service will make. If the service determines that a change larger than this is required, it logs an event instead.	54,000 (15 hrs)
MaxPosPhaseCorrection	The largest positive time correction in seconds that the service will make. If the service determines a change larger than this is required, it will log an event instead.	54,000 (15 hrs)
PhaseCorrectRate	One over how much of the remaining phase error in order to	7

	correct this update interval.	
PollAdjustFactor	Controls the decision to increase or decrease the poll interval for the system. The larger the value, the smaller the amount of error that causes the poll interval to be decreased.	5
SpikeWatchPeriod	The amount of time that a suspicious offset must persist before it is accepted as correct (in seconds).	90
UpdateInterval	The number of clock ticks between phase correction adjustments.	100
AnnounceFlags	Controls whether this computer is marked as a reliable time server. A computer is not marked as reliable unless it is also marked as a time server.	6
EventLogFlags	Controls the events that the time service logs.	2
LocalClockDispersion	The dispersion (in seconds) that you must assume when the only time source is the built-in complementary metal oxide semiconductor (CMOS) clock.	10
MaxPollInterval	The largest interval, in log2 seconds, allowed for the system polling interval. Note that while a system must poll according to the scheduled interval, a provider can refuse to produce samples when requested to do so.	15
MinPollInterval	The smallest interval, in log2 seconds, allowed for the system polling interval. Note that while a system does not request samples more frequently than this, a provider can produce samples at times other than the scheduled interval.	4

You can set the Windows NTP Client configuration settings for the Windows Time service by using Group Policy. For details about locating the Windows Time service policy settings, see "Procedures for configuring the Windows Time service" later in this section. The following table describes the settings.

Group Policy settings for configuring the Windows Time service NTP Client for computers running Windows XP

Policy setting	Effect of setting	Default setting
NtpServer	Establishes a space-delimited list of peers from which a computer obtains time stamps, consisting of one or more DNS names or IP addresses per line. Computers connected to a domain must synchronize with a more reliable time source, such as the official U.S. time clock.	time.microsoft.com
Type	Indicates which peers to accept synchronization from: **NoSync**. The time service does not synchronize with other sources. **NTP**. The time service synchronizes from the servers specified in the NtpServer registry entry. **NT5DS**. The time service synchronizes from the domain hierarchy. **AllSync**. The time service uses all the available synchronization mechanisms.	Default options **NTP**. Use on computers that are not joined to a domain. **NT5DS**. Use on computers that are joined to a domain.
CrossSiteSyncFlags	Determines whether the service chooses synchronization partners outside the domain of the computer.	2

	None 0 PdcOnly 1 All 2 This value is ignored if the NT5DS value is not set.	
ResolvePeerBackoffMinutes	Specifies the initial interval to wait, in minutes, before attempting to locate a peer to synchronize with.	15
ResolvePeerBackoffMaxTimes	Specifies the maximum number of times to double the wait interval when repeated attempts to locate a peer to synchronize with fail. A value of zero means that the wait interval is always the minimum.	7
EventLogFlags	Controls the events that the time service logs.	0

Notes

Group Policy for computers running Windows 2000 does not support managing the Windows Time service configuration settings. You will need to import the necessary Group Policy Administrative Templates to use Group Policy on a computer running Windows 2000 to manage the Windows Time service configuration settings. For more information about importing Group Policy Administrative Templates, see Appendix C, "Importing Group Policy settings for Windows XP to a server running Windows 2000 SP3."

Group Policy and Active Directory are tools that are available for controlling and managing computers and services within an enterprise or organization. The full description of the rich feature set and methods for using Group Policy are beyond the intended scope of this document. For other sources of information about Group Policy, see Appendix B, "Resources for learning about Group Policy."

For more information about the Windows Time service and the registry, see "Registry Entries for the W32Time Service" on the Microsoft Web site at:

support.microsoft.com/default.aspx?scid=kb;en-us;Q223184

Notes

To perform this procedure, you must be a member of the Administrators group on the local computer, or you must have been delegated the appropriate authority. If the computer is joined to a domain, members of the Domain Admins group may be able to perform this procedure. As a security best practice, consider using Run as to perform this procedure.

To open Registry Editor, click **Start**, click **Run**, and then type **regedit**.

The computer registry values for Windows 2000 listed in this section of the article are located in the following registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters

Registry settings for Windows Time service on Windows 2000 computers

Entry name	Data type	Description and values
ReliableTimeSource	REG_DWORD optional	Used to indicate that this computer has reliable time. 0 = Do not mark computer as reliable. [default = 0] 1 = Mark computer as reliable. This is only useful on a domain

		controller.
Period	REG_DWORD or REG_SZ	Used to control how often the time service synchronizes. If a value is given, it must be one of the special values listed below. 65531, "DailySpecialSkew" = once every 45 minutes until successful one time, then once every day 65532, "SpecialSkew" = once every 45 minutes until successful three times, then once every eight hours (three times per day) [default] 65533, "Weekly" = once every week (seven days) 65534, "Tridaily" = once every three days 65535, "BiDaily" = once every two days 0 = once per day freq = freq times per day. If you choose to add a value other than any of those specified above, you must use this option.
AvoidTimeSyncOnWan	REG_DWORD optional	Used to prevent the computer from synchronizing from a computer that is in another site and thus connected by a costly temporary connection. 0 = The site of the time source is ignored. [default = 0] 1 = The computer will not synchronize with a time source that is in a different site.
LocalNTP	REG_DWORD	Used to start the SNTP server. 0 = Do not start server unless this computer is a domain controller. [default = 0] 1 = Always start server.
Type	REG_SZ	Used to control how a computer synchronizes. Nt5DS = Synchronize to domain hierarchy or manually configured source. [default = Nt5DS] NTP = Synchronize to manually configured source. NoSync = Do not synchronize.
NtpServer	REG_SZ optional	Used to manually configure the time source. This can be set to the DNS name or IP address of the server from which to synchronize. Only one DNS name or IP address can be specified. This can be modified from the command line. [default = blank]
GetDcBackoffMinutes	REG_DWORD optional	The initial number of minutes to wait before looking for a domain controller (time source) if the last attempt to find a domain controller failed. [default = 15]
GetDcBackoffMaxTimes	REG_DWORD optional	The maximum number of times to double the backoff interval when successive attempts to find a domain controller fail. An event is logged every time a wait of the maximum length occurs. If the value of this entry is 0, then the wait between successive attempts is always the minimum and no event is logged. [default = 7] The time service tries to find a domain controller according to its usual synchronization schedule, but if the backoff interval has not expired, then that attempt will be skipped. For example, if given the default values, the backoff interval will follow this pattern: 15 minutes, 30 minutes, 1 hour, 2 hours, 4 hours, 8 hours, 16 hours, etc. The time service will, however, only attempt to synchronize on 45-minute intervals, so the attempts to find a domain controller will actually occur after 45 minutes, 1 hour 30 minutes, 2 hours 15 minutes, 4 hours 30 minutes, 8 hours 15 minutes, 16 hours 30 minutes, etc.

Caution Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on the computer. You can also use the Last Known Good Configuration startup option if you encounter problems after manual changes have been applied.

Procedures for configuring the Windows Time service

The following procedures explain how to set Windows Time Service configuration settings through Group Policy to achieve the configurations described in the previous subsections.

To set Group Policy for the Windows Time Service global configuration settings

1. Ensure that you have upgraded to the latest Administrative Template files. For more information, see Appendix C, "Importing Group Policy settings for Windows XP to a server running Windows 2000 SP3."
2. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.
   For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for learning about Group Policy."
3. Click **Computer Configuration**, click **Administrative Templates**, click **System**, and then click **Windows Time Service**.
4. In the details pane, double-click **Global Configuration Settings**, and then click **Enable**.

To configure the Group Policy setting to prevent your Windows XP computer from synchronizing its computer clock with other NTP servers

1. Ensure that you have upgraded to the latest Administrative Template files. For more information, see Appendix C, "Importing Group Policy settings for Windows XP to a server running Windows 2000 SP3."
2. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.
   For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for learning about Group Policy."
3. Click **Computer Configuration**, click **Administrative Templates**, click **System**, click **Windows Time Service**, and then click **Time Providers**.
4. In the details pane, double-click **Enable Windows NTP Client** and then select **Disabled**.

To configure the Group Policy setting to prevent your Windows XP computer from synchronizing its computer clock from the domain hierarchy or a manually configured NTP server

1. Ensure that you have upgraded to the latest Administrative Template files. For more information, see Appendix C, "Importing Group Policy settings for Windows XP to a server running Windows 2000 SP3."
2. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.
   For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for learning about Group Policy."
3. Click **Computer Configuration**, click **Administrative Templates**, click **System**, click **Windows Time Service**, and then click **Time Providers**.

4. In the details pane, double-click **Configure Windows NTP Client**, and then select **Disabled**.

To configure the Group Policy setting to prevent your Windows XP computer from servicing time synchronization requests from other computers on the network

1. Ensure that you have upgraded to the latest Administrative Template files. For more information, see Appendix C, "Importing Group Policy settings for Windows XP to a server running Windows 2000 SP3."
2. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.
   For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for learning about Group Policy."
3. Click **Computer Configuration**, click **Administrative Templates**, click **System**, click **Windows Time Service**, and then click **Time Providers**.
4. In the details pane, double-click **Enable Windows NTP Server**, and then select **Disabled**.

Starting and Stopping the Windows Time service

By default, the Windows Time service starts automatically at system startup. You can, however, start or stop the service manually by accessing services in Administrative Tools or by using the Net Time tool.

To manually start the Windows Time service using the graphical interface

1. Click **Start**, and then either click **Control Panel**, or point to **Settings** and then click **Control Panel**.
2. Double-click **Administrative Tools**, and then double-click **Services**.
3. Select **Windows Time** from the list of services.
4. On the **Action** menu, click **Start** to begin the service.

To manually stop the Windows Time service using the graphical interface

1. Click **Start**, and then either click **Control Panel**, or point to **Settings** and then click **Control Panel**.
2. Double-click **Administrative Tools**, and then double-click **Services**.
3. Select **Windows Time** from the list of services.
4. On the **Action** menu, click **Stop** to discontinue the service.

To manually start the Windows Time service using Net Time

1. Open Command Prompt.
2. At the command prompt, type **net start w32time,** and then press ENTER.

To manually stop the Windows Time service using Net Time

1. Open Command Prompt.
2. At the command prompt, type **net stop w32time,** and then press ENTER.

Synchronizing the internal time server with an external time source

To synchronize an internal time server with an external time source

1. Open command prompt:
2. Type the following, where *PeerList* is a comma-separated list of Domain Name System (DNS) names or Internet protocol (IP) addresses of the desired time sources:
   At the command prompt, type **w32tm /config /syncfromflags:manual /manualpeerlist:***PeerList,* and then press ENTER.
3. At the command prompt, type **w32tm /config /update,** and then press ENTER.

Notes
The most common use of this procedure is to synchronize the internal network's authoritative time source with precise external time source. This procedure, however, can be run on any computer running Windows XP.

If the computer cannot reach the servers, the procedure fails and an entry is written to the Windows System event log.

To synchronize the client time with a time server

1. Open Command Prompt.
2. At the command prompt, type **w32tm /resync**, and then press ENTER.

Notes
This procedure only works on computers that are joined to a domain.

The W32tm tool is used for diagnosing problems that can occur with the Windows Time service. If you are going to use the W32tm tool on a domain controller, it is necessary to stop the service. Running W32tm and the Windows Time service at the same time on a domain controller generates an error because both are attempting to use the same UDP port. When you finish using W32tm, the service must be restarted.

Monitoring and troubleshooting the Windows Time service

In many cases problems with the Windows Time service can be attributed to network configuration. If the network is not configured correctly computers might not be able to communicate to send time samples back and forth. Viewing the contents of NTP packets can help you to identify exactly where a packet is blocked on a network. An error associated with the Windows Time service might occur when a computer is unable to synchronize with an authoritative source. You can use the W32tm command-line tool to assist you in troubleshooting this and other types of errors associated with the Windows Time service.

W32tm.exe is the preferred command-line tool for configuring, monitoring, and troubleshooting the Windows Time service. All tasks that can be performed by using the net time command can be accomplished by using W32tm.exe or Group Policy. For more information, look up "W32tm" in the Windows Help index.

Procedure to follow when a computer is unable to synchronize

A computer running the Windows Time service refuses to synchronize if the computer's time is more than 15 hours off. Such occurrences are rare, and are often caused by configuration setting errors. For example, if a user sets the date on the computer incorrectly, the time does not synchronize. Under these circumstances, most often the time is off by a day or more. Be sure to check the computer's calendar and ensure that the correct date has been set.

To resynchronize the client time with a time server

1. Click **Start**, point to **All Programs**, point to **Accessories**, and then click **Command Prompt**.
2. At the command prompt, type **w32tm /resync /rediscover**, and then press ENTER.

Notes
When you run the preceding command, it redetects the network configuration and rediscovers network resources, causing resynchronization. This procedure only works on computers that are joined to a domain. You can then view the event log for more information about why the time service does not synchronize. For more information, look up "Monitoring and controlling services on computers" in the Windows Help index.

The W32tm tool is used for diagnosing problems that can occur with the Windows Time service. If you are going to use the W32tm tool on a domain controller, it is necessary to stop the service. Running W32tm and the Windows Time service at the same time on a domain controller generates an error because both are attempting to use the same UDP port. When you finish using W32tm, the service must be restarted.

Related Links

- For more information about the Windows Time service, see the following pages on the Microsoft Web site at:

  www.microsoft.com/windows2000/techinfo/howitworks/security/wintimeserv.asp

  www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/maintain/operate/wintime.asp

- For more information about the Windows Time service and the registry, see "Registry Entries for the W32Time Service" on the Microsoft Web site at:

  support.microsoft.com/default.aspx?scid=kb;en-us;Q223184

- For more information about importing Group Policy Administrative Templates, see Appendix C, "Importing Group Policy settings for Windows XP to a server running Windows 2000 SP3."

Using online resources. The Microsoft Web site contains support information, including the latest downloads and Knowledge Base articles written by support professionals at Microsoft:

- You can search frequently asked questions (FAQs) by product, browse the product support newsgroups, and contact Microsoft Support at the following Web site. You can also search the Microsoft Knowledge Base of technical support information and self-help tools for Microsoft products at this site:

  support.microsoft.com/

- You can search for troubleshooting information, service packs, patches, and downloads for your system on the Technet Web site at

  www.microsoft.com/technet/

Windows Update and Automatic Update

The following sections provide information about:

- The benefits of Windows Update and Automatic Update
- How Windows Update and Automatic Update communicate with sites on the Internet
- How to control Windows Update and Automatic Update to limit the flow of information to and from the Internet

Benefits and purposes of Windows Update and Automatic Update

Windows Update

Windows Update is an online catalog customized for computers running Microsoft Windows XP Professional Service Pack 1 (SP1) that consists of items such as drivers, critical updates, Help files, and Internet products. Windows Update scans the user's computer and provides a tailored selection of updates that apply only to the software and hardware on that specific computer. Windows Update then enables users to choose updates for their computer's operating system and hardware. New content is added to the Windows Update Web site regularly, so users can always get the most recent and secure updates and solutions.

Windows Update contains two key components:

- **Content update**: Content updates occur when the user accesses the Windows Update Web site and selects component updates to download and install. The user is fully aware of downloads to the computer. The Windows Update Web site is at:

  windowsupdate.microsoft.com/

- **Web service control update**: The Windows Update Web service includes an ActiveX Web control program that downloads and installs the content updates. The Windows Update team receives feedback from their customers on how to improve their Web service and the Windows Update service control is changed to reflect the needs of the customers. In order to access the new content and services customers need, the Web controls are updated periodically. This service automatically downloads a new version of the Web control program when the user visits the Windows Update site or when any of the other Windows features calls on the Windows Update control. Just like downloading an ActiveX control, the user may receive a security dialog box that a Web control is attempting to be installed. Users may not receive the dialog box if they have selected to always trust Microsoft as a content provider (using their security settings in Microsoft Internet Explorer). If users do not click Yes on the security dialog box, the control will not be updated.

Automatic Update

This option for updating a computer allows for updates without interrupting the user's Web experience. Automatic Update is not enabled by default; users are prompted to enable this option following Setup. When Automatic Update is enabled, users do not need to visit special Web pages or remember to periodically check for new updates. An icon appears in the notification area each time new updates are available. Updates can be downloaded in the background with minimal impact on the user's network connections. Once the update is downloaded, Windows XP prompts the user to install it. Users can set

Automatic Update options in one of three ways to control how and when they want Windows XP to update their computers. They can:

- Choose to have Windows XP send a notification before downloading and installing any updates.
- Choose to have Windows XP download and install updates automatically on a schedule that they specify.
- Choose to have Windows XP send a notification whenever it finds updates available for their computers; Windows XP will then download the updates in the background, enabling users to continue working uninterrupted. After the download is complete, an icon in the notification area will prompt users that the updates are ready to be installed.

Users can choose not to install a specific update that has been downloaded; in that case, Windows XP will delete those files from the computer. Users can download those deleted files again by opening the Performance and Maintenance category in Control Panel, clicking the System tool, clicking the Automatic Updates tab, and then clicking Declined Updates. (In Control Panel's Classic View, you can open the System tool directly from Control Panel). If any of the updates users previously declined can still be applied to their computers, they will appear the next time Windows XP notifies those users of available updates.

Alternatives to Windows Update and Automatic Update

For managed environments, there are three alternatives to Windows Update:

- Windows Update Catalog Web site.
- Microsoft Software Update Services (SUS).
- Distribution software, such as Microsoft Systems Management Server, that can be used to distribute software updates. For more information, see the documentation for your distribution software, and see Appendix A, "Resources for learning about automated installation and deployment," especially the "Related Documentation and Links" subsection in that appendix.

Windows Update Catalog Web Site

You can deploy updates to Windows in a managed environment without requiring users to connect to the Windows Update Web site by using the Windows Update Catalog site, located at:

corporate.windowsupdate.microsoft.com

The Windows Update Catalog site provides a comprehensive catalog of updates that can be distributed over a managed network. It provides a single location for Windows Update content and drivers that display the Designed for Windows logo. Administrators can search the site using keywords or predefined search criteria to select the relevant downloads and to download the updates to a location on their internal network.

For additional information about using the Windows Update Corporate site, see the Microsoft Web site at:

www.microsoft.com/windowsxp/pro/techinfo/deployment/planning/default.asp

Microsoft Software Update Services (SUS)

Microsoft Software Update Services (SUS) is a version of Windows Update designed for installation inside an organization's firewall. This feature is very useful for organizations that:

- Do not want their systems or users connecting to an external Web site
- Want to first test these updates before deploying them throughout their organizations

Microsoft Software Update Services enables administrators to quickly and reliably deploy critical updates to their Windows 2000-based servers as well as desktop computers running Windows 2000 Professional or Windows XP Professional.

For more information about software update services, see the Microsoft Web site at:

www.microsoft.com/windows2000/windowsupdate/sus/default.asp

Overview: Using Windows Update and Automatic Update in a managed environment

Users have control over whether to enable Automatic Update following Setup and also have direct control over Windows Update. In a managed environment, however, it is unlikely that users will be allowed unlimited access to install updated drivers and other updated files; this function would normally be controlled in some fashion by the IT department. You can use Group Policy to disable both Windows Update and Automatic Update and to block users from accessing Windows Update in the user interface. You can also disable Automatic Update using the System tool in Control Panel. Details on the methods and procedures for controlling these features are described in the following subsections.

How Windows Update and Automatic Update communicate with sites on the Internet

This subsection summarizes the communication process:

- **Specific information sent or received**: Drivers and replacement files (critical updates, Help files, and Internet products) may be downloaded to the user’s computer. The computer is uniquely identified and is logged in the download/installation success report, but the user is not uniquely identified.
- **Default and recommended settings**: By default, Windows XP allows access to the Windows Update Web site. Recommended settings are described in the next subsection, "Controlling Windows Update and Automatic Update to limit the flow of information to and from the Internet."
- **Triggers**: The user controls whether to run Windows Update. If Automatic Update is enabled following Setup, it is triggered about once per day when there is an Internet connection.
- **User notification**:
    - **Windows Update**: Users are notified when Windows Update downloads files to their computers, and they have control over whether to install those downloads.
    - **Automatic Update**: Administrators can specify one of two notification settings for Automatic Update:
        - Notify users before downloading and installing any updates.
        - Download the updates automatically and notify users when they are ready to be installed.

    Note Administrators can also specify that updates be automatically downloaded and installed following a set schedule without user notification. For more information about these settings, see the topic titled "To change settings for automatic updating" in Help and Support Center.

- **Logging**: Automatic Updates logs events to the event log.

- **Encryption**: The data is transferred using HTTPS. The data packages downloaded to the user's system by Microsoft are digitally signed.
- **Privacy policy**: To view the privacy policy for Windows Update, see the Windows Update Web site, click About Windows Update, and scroll down until you see the heading Windows Update Privacy Statement. The Windows Update Web site is located at:

  windowsupdate.microsoft.com/

  Automatic Update is covered by the same policy that covers Windows Update.
- **Transmission protocol and port**: The transmission protocols and ports used are HTTP 80 and HTTPS 443.
- **Ability to disable**: You can use Group Policy to prohibit Windows XP from searching for updates, thereby blocking both Windows Update and Automatic Update, and to remove user access to Windows Update in the user interface. You can disable Automatic Update using Control Panel tools. Procedures for these methods are given at the end of this section.

Controlling Windows Update and Automatic Update to limit the flow of information to and from the Internet

You can use Group Policy settings to control Windows Update and Automatic Update by:

- Prohibiting Windows XP from searching for and downloading updates
- Removing end user access to Windows Update

You can use System settings in Control Panel to selectively disable Automatic Update.

Alternatively, you can control both Windows Update and Automatic Update by blocking HTTP port 80 or HTTPS port 443 or both at the firewall.

See the following table for more information about the configuration options.

Configuration settings for Windows Update and Automatic Update

Automatic Update: Configuration tool	**Setting**	**Result**
Control Panel (System tool)	On the **Automatic Updates** tab, clear **Keep my computer up to date**.	Disables Automatic Update.
Windows Update and Automatic Update: Configuration tool	**Setting**	**Result**
Firewall	Block HTTP port 80 or HTTPS port 443 or both.	Blocks Windows Update and Automatic Update.
Group Policy	Disable the **Windows Automatic Updates** policy setting in the System.adm Group Policy template. For more information, see "Procedures for disabling Windows Update and Automatic Update" later in this section.	Blocks Windows Update and Automatic Update (prevents Windows XP from searching for updates).
Group Policy	Enable the **Remove access to use all Windows Update features** policy setting in the Wuau.adm Group Policy template. For	Blocks the user from accessing Windows Update in the Windows XP user interface. Also blocks Automatic

	more information, see "Procedures for disabling Windows Update and Automatic Update" later in this section.	Update.

How controlling Windows Update and Automatic Update can affect users and applications

When you use Group Policy to prohibit Windows XP from searching for and downloading updates, you will block both Windows Update and Automatic Update.

When you remove user access to Windows Update, Windows will still search for and download updates to the local computer. Users will not, however, be able to access the Windows Update Web site from the Windows Update hyperlink on the Start menu (by clicking **Start**, then **All Programs**, and then **Windows Update**), or from the Tools menu in Microsoft Internet Explorer. They will also not be prompted to install downloaded updates. In addition, removing user access to Windows Update also disables Automatic Update; that is, the user for which this policy setting is enabled will neither be notified about nor will receive critical updates from Windows Update. Removing user access to Windows Update is a user-based, not system-based, policy; other users on the same computer will still receive critical updates unless this policy setting is also enabled for those users individually.

Removing end user access to Windows Update also prevents Device Manager from automatically installing driver updates from the Windows Update Web site. For more information about controlling Device Manager, see the section of this white paper titled "Device Manager."

Blocking Windows Update and Automatic Update will not block applications from running.

The Windows Update site is located at:

windowsupdate.microsoft.com/

Procedures for disabling Windows Update and Automatic Update

You can use Group Policy to prevent Windows XP from searching for updates. This will block both Windows Update and Automatic Update.

To disable Windows Update and Automatic Update using Group Policy

1. Ensure that you have upgraded to the administrative template System.adm. For more information, see Appendix C, "Importing Group Policy settings for Windows XP to a server running Windows 2000 SP3."
2. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.
   For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for learning about Group Policy."
3. Click **User Configuration**, click **Administrative Templates**, and then click **System**.
4. In the details pane, double-click **Windows Automatic Updates**, and then click **Enabled**.

   Note If you disable or do not configure this setting, Windows XP searches for updates and automatically downloads them.

You can remove user access to Windows Update by using Group Policy. This will also block Automatic Update.

To remove user access to Windows Update using Group Policy

1. Ensure that you have upgraded to the administrative template Wuau.adm. For more information, see Appendix C, "Importing Group Policy settings for Windows XP to a server running Windows 2000 SP3."
2. On a server running Windows 2000, follow the instructions in Help for opening Group Policy in the appropriate way, depending on whether you want to apply the Group Policy object (GPO) to an organizational unit, a domain, or a site.
For more information about Group Policy or about viewing information about Group Policy in Windows 2000 Help, see Appendix B, "Resources for learning about Group Policy."
3. Click **User Configuration**, click **Administrative Templates**, click **Windows Components**, and then click **Windows Update**.
4. In the details pane, double-click **Remove access to use all Windows Update features**, and then click **Enabled**.

Important Removing user access to Windows Update also disables Automatic Update.

You can disable Automatic Update by using the Control Panel tools or Group Policy.

To disable Automatic Update using Control Panel tools

1. Click **Start**, and then either click **Control Panel**, or point to **Settings** and then click **Control Panel**.
2. On the **Automatic Updates** tab, clear the **Keep my computer up to date** check box.

Appendices

Appendix A: Resources for learning about automated installation and deployment

The following appendix provides:

- An overview of automated installation and deployment
- Procedures and resources for obtaining more information about automated installation and deployment

Overview: Automated installation and deployment

In the enterprise environment, it is not cost-effective to install Microsoft Windows 2000 or Microsoft Windows XP Professional Service Pack 1 (SP1) using the standard interactive setup on each computer. To greatly lower the total cost of ownership (TCO) and ensure configuration uniformity, you can perform an automated installation of Windows 2000 Server and Windows XP on multiple computers. By using an automated installation method, you can ensure that certain components and applications are not available on your organization’s computers, or that certain components and applications are preconfigured in such a way that helps prevent unwanted communication over the Internet.

Notes
In addition to the automated installation methods described here, another common method of controlling Internet connections is to use a script to configure Group Policy on each client computer. The script can be sent to each client computer using a tool such as Microsoft Systems Management Server and can run remotely using Windows Script Host. Alternatively, Group Policy can be applied to a domain, site, or organizational unit. The policy settings would then automatically be applied to every computer in the domain, site, or organizational unit the first time the computer starts after the operating system is installed. For more information about scripts and Group Policy, see "Related Documentation and Links" at the end of this section.

You can also use scripts to monitor activity on client computers and to take appropriate action if certain restricted activities occur. For example, if a user were to start an unauthorized application, a script could be used to detect this and to immediately stop that application. Similarly, scripts can be used to monitor the setup of each computer in order to, for example, determine what applications are installed and what folders are being shared. Configuring these scripts is beyond the scope of this document; however, you can refer to "Related Documentation and Links" at the end of this section for more information.

There are several options for automating the setup process. Any or all of the following tools can help ensure that all of your client computers are configured to appropriately limit communication over the Internet:

- Unattended setup using Setup (Winnt32.exe)

  Unattended setup enables you to simplify the process of setting up the operating system on multiple computers by running Setup unattended. To do this, you can create and use an answer file, which is a customized script that answers Setup questions automatically. Then you can run Setup (Winnt32.exe) from the command line with the appropriate options for invoking unattended setup.

  Using Winnt32.exe, you can upgrade your previous version of the operating system using all user settings from the previous installation, or you can perform a fresh installation using the answer file that provides Setup with your custom specifications. The latter method is most likely the best option to limit component communication over the Internet, provided you use an appropriate answer file. Details about specific answer file entries are included in the appropriate component sections of this white paper.

- Remote Installation Services (RIS)

  You can use RIS to create installation images of operating systems or of complete computer configurations, including desktop settings and applications. You can then make these installation images available to users at client computers. You can also specify which RIS server will provide installations to a given client computer, or you can allow any RIS server to provide the installation.

- Image-based installation using the System Preparation (Sysprep) tool.

  Image-based installation is also a good choice if you need to install an identical configuration on multiple computers. On a master computer, you install the operating system and any applications that you want installed on all of the target computers. Then you run Sysprep and a disk imaging utility. Sysprep prepares the hard disk on the master computer so that the disk imaging utility can transfer an image of the hard disk to the other computers. This method decreases deployment time dramatically compared to standard or scripted installations. The image can be packaged and compressed, and only the files required for the specific configuration are created as part of the image. Additional Plug and Play drivers that you might need on other systems are also created. The image can also be copied to a CD and distributed to remote sites that have slow links.

- System management software, such as Microsoft Systems Management Server (SMS)

  This software assists with the many tasks that are involved when you apply automated procedures to multiple servers and client computers throughout your organization. These tasks include:

  - Selecting computers that are equipped for the operating system and that you are ready to support.
  - Distributing the operating system source files to all sites, including remote sites and sites without technical support staff.
  - Monitoring the distribution to all sites.
  - Securely providing the appropriate user rights to do the upgrade.
  - Automatically initiating the installation of the software package with the possibility of having the user control the timing.
  - Resolving problems related to the distributions or installations.
  - Reporting on the rate and success of deployment.

Using system management software, you can further ensure that all computers within your organization have received the standardized operating system configuration that helps prevent unwanted communication over the Internet.

Procedures for accessing additional information about other automated setup tools

Accessing the Windows 2000 Help documentation

Windows 2000 has Help documentation describing unattended installation, RIS, and image-based installation. You can view this documentation from any computer that has Internet access (regardless of the operating system running on that computer), or from any server running Windows 2000. The following procedure gives the details.

To access the Help documentation on a server running Windows 2000

1. Open Help for a Windows 2000 server product by doing one of the following:

   - On any computer running Windows 2000 Server, Windows 2000 Advanced Server or Windows 2000 Datacenter Server, click **Start,** and then click **Help.** Click the **Contents** tab. If the **Contents** tab is not showing, click **Show,** and then click the **Contents** tab.

   - View Help on the Web at:

     www.microsoft.com/windows2000/techinfo/proddoc/

2. Locate the specific topics as follows:

   - For unattended installation: Navigate to Getting Started with Windows 2000 Server\Installing Windows 2000 Server\Concepts\Planning for unattended setup.

   - For RIS: Navigate to Users and Computers\Remote Installation Services.

Related Documentation and Links

You can also find additional information about all of the topics described earlier in this appendix in a variety of other locations:

- On the Windows XP CD, you can find additional information about unattended installations in Deploy.chm in \Support\Tools\deploy.cab.

- The Windows 2000 Help documentation on the Web includes information about Winnt32.exe at:

  www.microsoft.com/windows2000/en/advanced/help/wgs_gs_03016.htm

- For extensive information about unattended setup and Systems Management Server, see the following topics in the Windows 2000 Resource Kit on the Web:

  - "Automating Server Installation and Upgrade" at: www.microsoft.com/windows2000/techinfo/reskit/en-us/deploy/dgcb_ins_adeb.asp

  - "Using Systems Management Server to Deploy Windows 2000" at: www.microsoft.com/windows2000/techinfo/reskit/en-us/deploy/dggf_sms_zunm.asp

- Information about automated and customized installations can also be found in the Windows XP Resource Kit on the Web at:

  www.microsoft.com/technet/prodtechnol/winxppro/reskit/prbc_cai_nmip.asp

- For general information about Group Policy, see Appendix B, "Resources for learning about Group Policy" and Appendix C, "Importing Group Policy settings for Windows XP to a server running Windows 2000 SP3."

- To learn about specific Group Policy settings that can be applied to computers running Windows XP Professional SP1, see the spreadsheet titled "Windows XP Professional Resource Kit, Group Policy Object Settings" at:

  www.microsoft.com/WindowsXP/pro/techinfo/productdoc/gpss.asp

- The Windows 2000 Help documentation included on the CD and on the Web includes information about Windows Script Host. You can find the documentation on the Web at:

  www.microsoft.com/windows2000/en/advanced/help/sag_WSHtopnode.htm

Appendix B: Resources for learning about Group Policy

The following appendix provides:

- An overview of Group Policy
- Procedures for obtaining more information about Group Policy

Overview: Group Policy

As described in earlier sections of this white paper, you can use Group Policy to configure many Windows XP Professional Service Pack 1 (SP1) components in a way that will prevent users from accessing these components, or alternatively, in a way that will control how these components exchange data over the Internet. Group Policy settings define the various aspects of the user's desktop environment that a system administrator can manage; for example, the applications that are available to users and how those applications operate.

Group Policy includes **User Configuration** policy settings, which affect users, and **Computer Configuration** policy settings, which affect computers. Using Group Policy you can, among other tasks:

- Make certain Windows components unavailable to particular users.
- Assign scripts (such as computer startup and shutdown, and logon and logoff).
- Specify security options.
- Manage registry-based policy through Administrative Templates. Group Policy creates a file that contains registry settings that are written to the User or Local Machine portion of the registry database. User profile settings that are specific to a user who logs on to a given workstation or server are written to the registry under HKEY_CURRENT_USER (HKCU). Computer-specific settings are written under HKEY_LOCAL_MACHINE (HKLM).

How and when Group Policy is applied

User policy settings are obtained when a user logs on. Computer policy settings and are obtained when a computer boots.

Order of application

Policy settings are applied in this order:

1. The unique local Group Policy object (GPO). (A GPO is a collection of policy settings.)
2. Group Policy objects for sites, in administratively specified order.
3. Group Policy objects for domains, in administratively specified order.
4. Group Policy objects for organizational units, from the largest to the smallest organizational unit (parent to child organizational unit), and in administratively specified order at the level of each organizational unit.

By default, policy settings applied later overwrite previously applied policy settings when there is an inconsistency. If the policy settings are not inconsistent, however, earlier and later policy settings both contribute to the effective policy.

Blocking policy inheritance

Policy settings that would otherwise be inherited from higher site, domain, or organizational units can be blocked at the site, domain, or organizational unit level.

Enforcing policy from above

Policy settings that would otherwise be overwritten by policy settings in child organizational units can be set to **No Override** at the Group Policy object level. Policy settings set to **No Override** cannot be blocked.

Procedures for accessing additional information about Group Policy

Accessing the Group Policy Help documentation for Windows 2000

Windows 2000 has extensive Help documentation describing Group Policy concepts and procedures. You can view this documentation from any computer that has Internet access (regardless of the operating system running on that computer), or from any server running Windows 2000. The following procedure describes details.

To view Group Policy Help documentation for servers running Windows 2000

1. Open Help for a Windows 2000 server product by doing one of the following:
   - On any computer running Windows 2000 Server, Windows 2000 Advanced Server or Windows 2000 Datacenter Server, click **Start,** and then click **Help.** Click the **Contents** tab. If the **Contents** tab is not showing, click **Show**, and then click the **Contents** tab.
   - View Help on the Web at:

     www.microsoft.com/windows2000/techinfo/proddoc/
2. Double-click **Users and Computers**.
3. Double-click **Group Policy**.

Related Links

For more information about Group Policy, see the following references:

- "Windows 2000 Group Policy Reference" in the Windows 2000 Resource Kit at:

  www.microsoft.com/windows2000/techinfo/reskit/en-us/w2rkbook/gp.asp
- "Using Group Policy to Manage Desktops" in the Windows XP Professional Resource Kit (Part II, Chapter 5, "Managing Desktops") at:

Using Windows XP Professional with Service Pack 1 in a Managed Environment

www.microsoft.com/technet/prodtechnol/winxppro/reskit/prda_dcm_jplq.asp

To learn about specific Group Policy settings that can be applied to computers running Microsoft Windows XP Service Pack 1 (SP1), see the spreadsheet titled, "Windows XP Professional Resource Kit, Group Policy Object Settings" at:

www.microsoft.com/WindowsXP/pro/techinfo/productdoc/gpss.asp

For information on how to create your own administrative templates for controlling application settings, see:

www.microsoft.com/windows2000/techinfo/howitworks/management/rbppaper.asp

Appendix C: Importing Group Policy settings for Windows XP to a server running Windows 2000 SP3

Microsoft Windows XP Professional Service Pack 1 (SP1) has many new policy settings beyond what are available in Windows 2000 Service Pack 3 (SP3). In order to configure Windows XP Group Policy settings from a server running Windows 2000, and to use those policy settings to manage Windows XP clients, you must first copy the Windows XP Administrative Templates to the server running Windows 2000.

> **Note** The policy settings that are included with Windows XP only work on computers running Windows XP and will be ignored by all computers running Windows 2000. Computers running Windows 2000 are not affected by any of the new policy settings that come with Windows XP.

The following appendix provides:

- An overview of Administrative Templates
- A procedure for upgrading to the latest Administrative Template files

Overview: Administrative Templates

Group Policy requires a source from which to generate the user interface settings that you as an administrator can set. For this purpose, Group Policy can use an encoded text file referred to as an Administrative Template (.adm file). The .adm file consists of a hierarchy of categories and subcategories that together define how the configuration options are displayed through Group Policy.

Windows XP contains the following updated Administrative Template files:

- System.adm: used for core settings.
- Wmplayer.adm: used for Windows Media Player settings.
- Conf.adm: used for NetMeeting conferencing software.
- Inetres.adm: used for Microsoft Internet Explorer.
- Wuau.adm: used for Windows Update.

In order to use Administrative Templates in Windows XP on a server running Windows 2000, you copy the .adm files from the computer running Windows XP and then add them to Administrative Templates on the server running Windows 2000.

Upgrading to the latest Administrative Template files

To upgrade .adm files on a server running Windows 2000 to include Windows XP policy settings

1. On a computer running Windows XP, navigate to the **WINNT/INF** folder, which contains the Windows XP .adm files.
2. Copy system.adm and any of the other .adm files that you need (depending on which components you want to configure) to a shared folder.

3. Go to a server running Windows 2000 and open a Group Policy object (GPO) using the Group Policy Object Editor. For more information about how to do this, see Appendix B, "Resources for learning about Group Policy," which contains instructions for accessing the Group Policy Help documentation.
4. Right-click **Administrative Templates** under either **User Configuration** or **Computer Configuration** (it does not matter which one) and select **Add/Remove Templates**.
5. In the **Add/Remove Templates** dialog box, remove the Windows 2000-based .adm files.
6. Still in the **Add/Remove Templates** dialog box, add the Windows XP-based .adm files from the shared folder.
7. Repeat this procedure for each GPO.

Notes
Consider the following when using Administrative Templates:

In a mixed environment, use Windows XP .adm files to administer your GPOs.

Try to apply the same policy settings to both Windows XP and Windows 2000 so that roaming users can have a consistent experience.

Test interoperability of the various policy settings before deployment.

Only configure policy settings on clients using GPOs. Do not try to create these registry values by other methods.

Related Links

For more information on managing Windows XP in a Windows 2000 Server environment, see the white paper at:

www.microsoft.com/windowsxp/pro/techinfo/administration/policy/default.asp

For more information on Group Policy, see Appendix B, "Resources for learning about Group Policy."

To learn about specific Group Policy settings that can be applied to computers running Windows XP Professional SP1, see the spreadsheet titled "Windows XP Professional Resource Kit, Group Policy Object Settings" at:

www.microsoft.com/WindowsXP/pro/techinfo/productdoc/gpss.asp

For information on how to create your own administrative templates for controlling application settings, see:

www.microsoft.com/windows2000/techinfo/howitworks/management/rbppaper.asp

Appendix D: Application Compatibility Toolkit

Benefits and purposes of the Application Compatibility Toolkit

The Application Compatibility Toolkit contains tools and documents to aid IT professionals in planning a deployment of Microsoft Windows XP Professional Service Pack 1 (SP1) or Windows 2000. These resources are also useful to developers writing compatible applications for these operating systems.

The Application Compatibility Toolkit is intended for IT administrators and developers. It is not automatically installed during the setup of the operating system. The information in this appendix is provided in order to make you aware of the toolkit, and to explain the Internet connections that it makes.

Using the Application Compatibility Toolkit

The following tools are included in the Application Compatibility Toolkit:

- Application Verifier (AppVerifier)
- Compatibility Administration Tool (CompatAdmin)
- Page Heap (PageHeap)
- Quick Fix Application (QFixApp)

Application Verifier

Application Verifier (AppVerifier) is a graphical user interface (GUI) tool that aids IT managers and developers in testing applications on Windows XP. It focuses on detecting the common issues that deal with application quality such as heap corruption, security vulnerabilities, and registry usage. The tool does this by monitoring an application's interaction with the operating system, and profiling its use of kernel objects, the registry, the file system, and Win32 application programming interfaces (APIs).

Compatibility Administration Tool

This administration tool provides a graphical user interface (GUI) for working with the compatibility data and features on Windows XP and Windows 2000 operating systems. You can turn on and off any of the internal system fixes, browse for fixed applications on system drives, fix application security issues that prevent older applications from working with accounts that are not in the Administrators group, and create multiple fix packages that can be propagated and installed on other computers to resolve compatibility issues.

Note The recommended process to follow when resolving application compatibility issues for Windows XP is to use Quick Fix Application to find and identify the compatibility modes or fixes that will solve the problem with a single application, and then use that information in the Compatibility Administrator application to create or modify a custom compatibility database file.

Page Heap

This command-line tool sets page heap flags that help to find heap-related bugs and corruption. It can also help detect leaks in applications that are running on Windows 2000 Professional SP2 and Windows XP Professional operating systems.

Page Heap introduces a software validation layer (Page Heap manager) between the application and the system that verifies all dynamic memory operations (memory allocations, memory freeing, and other heap operations). When Page Heap manager is enabled, there is an option to start the application being tested under a debugger. If a bug is encountered, it will cause a debugger break.

Quick Fix Application

This GUI tool provides an interface for determining which combination of fixes will resolve an application compatibility problem for a selected executable (.exe) file. When your target file has a common name (for example, setup.exe), Quick Fix Application provides the ability to identify a file using file properties and matching file information. This ensures that fixes are applied to the correct file. Once you have uniquely identified a target file, you can use Quick Fix Application to identify which combinations of fixes enable that application to work on Windows XP.

Installing the Application Compatibility Toolkit

The Application Compatibility Toolkit is installed over the Internet over port 80. You can install the latest version on Windows XP or on Windows 2000 SP3 or later by using the link at the following location:

www.microsoft.com/windowsxp/appexperience/default.asp

The Windows XP CD also includes the file ACT20.EXE in the \Support\Tools folder. This file will direct you to the latest version of the toolkit on the Internet.

When you first install the Application Compatibility Toolkit, you will be presented with an overview. You will also see a list of tools, documents, and online resources. From this overview, you can install any of the tools from this list and access any of the documentation. Many of the tools and documents listed in the overview make a connection to the Internet. See the next subsection for details of the communication process.

How the Application Compatibility Toolkit communicates with sites on the Internet

You must be connected to the Internet in order to install the Application Compatibility Toolkit. You should also be aware that both the tools and the documentation included in the toolkit can communicate over the Internet as described in this subsection. Due to the variety of potential Internet connections made by this toolkit, if you are on a computer or in an organization where you want to place strict limits on all communication with the Internet, you may want to limit its use.

Application Verifier and Compatibility Administration Tool

When you start either of these tools, you will be asked if you want to check for updates. If you select No, no connection over the Internet is made. If you select Yes, the tool makes a connection over the Internet to a Microsoft Web site. The tool uses an HTTP request over port 80 to get information from a text file stored on the Web server. This information is then stored in the client computer's memory. The information from that text file is used to compare the current version on the computer to the latest version available. If there is a newer version available, the tool informs the user that an update is available and displays a link that the user can use to manually download the updated files. Information is not sent from the client computer during the check for available updates.

Users can also request that this check for updates occur on a regular basis, or that they can manually initiate this process at any time when using the tool.

Page Heap and Quick Fix Application

These two applications do not make any connections over the Internet.

Documentation

The overview page that is displayed when you first open the Application Compatibility Toolkit contains several links to a variety of documents. Some of these documents must be accessed over the Internet. The links to these documents are all labeled with a globe icon 🌐. If you are connected to the Internet and click any of these links, you will link to the document on the Internet.

The overview page also includes a link to the Microsoft Application Compatibility Analyzer tool. This link will connect you to the Internet where you can download the tool (currently under development).

Appendix E: Internet Connection Sharing and Internet Connection Firewall

The Internet Connection Sharing and Internet Connection Firewall features of Microsoft Windows XP Professional Service Pack 1 (SP1) are designed for home and small office networks. Information about these features is presented here so you as an IT administrator can be aware of these potential capabilities within your organization's network when you install Windows XP SP1.

This appendix includes the following information:

- An overview of Internet Connection Sharing and Internet Connection Firewall.
- How Internet Connection Sharing and Internet Connection Firewall might be used in a large organization's network.
- How to control or prevent the use of Internet Connection Sharing and Internet Connection Firewall.

Overview: Internet Connection Sharing and Internet Connection Firewall

With Internet Connection Sharing (ICS), an administrator can connect computers on a home or small office network to the Internet using just one connection. For example, you might have one computer that connects to the Internet using a dial-up connection. When ICS is enabled on this computer, called the ICS host, other computers on the network can connect to the Internet through this dial-up connection.

Internet Connection Sharing is intended for use in a network where the ICS host computer directs network communication between computers and the Internet. It is assumed that in a home or small office network, the ICS host computer has the only Internet connection.

Internet Connection Firewall (ICF), used in conjunction with ICS, is firewall software that an administrator can use to set restrictions on what information is communicated from the Internet to your network.

> **Note** You should not use Internet Connection Sharing in an existing network with Windows 2000 Server domain controllers, DNS servers, gateways, DHCP servers, or systems configured for static IP addresses.

Using Internet Connection Sharing and Internet Connection Firewall in a managed environment

While Internet Connection Sharing (ICS) and Internet Connection Firewall (ICF) are designed for home and small office use, an administrator within a large network can set up Internet Connection Sharing on a single computer with a direct connection to the Internet. ICS lets administrators configure a computer as an Internet gateway for a small network, and it provides network services, such as name resolution and addressing through Dynamic Host Configuration Protocol (DHCP), to the local private network.

Using Internet Connection Firewall, an administrator can enable a firewall to protect the public connection of a small network or single computer that is connected to the Internet. ICF is considered a "stateful" firewall. A stateful firewall is one that monitors all aspects of the communications that cross its path and inspects the source and destination address of each message that it handles.

Any organization that uses domain controllers, DHCP, Domain Name System (DNS), and other elements of network infrastructure should not use ICS and ICF, but can instead use a firewall designed for the entire organization. There are instances, however, where a firewall on an individual user's computer reveals an unrecognized hole in the organization's firewall, specifically, when a dial-up connection used for checking e-mail creates an exploitable tunnel to an individual computer.

Because of vulnerabilities such as these, it is important to be aware of all the methods users have for connecting to your networked assets, and to review whether your security measures provide in-depth defense (as contrasted with a single layer of defense, more easily breached).

Both ICS and ICF are disabled by default, but an administrator can enable either or both of them by changing the settings of a network connection through Control Panel\Network Connections\Network Tasks. In a highly managed environment you might not want the capability to set up Internet Connection Sharing or an Internet Connection Firewall to be available.

Controlling the use of Internet Connection Sharing and Internet Connection Firewall

You can block administrators and users from accessing these features by using answer files during initial installation and Group Policy post-deployment. For Internet Connection Sharing, you can exclude the component during unattended installation by using an answer file. Or, if Windows XP SP1 has already been deployed in your organization, you can disable both ICS and ICF by using Group Policy.

Using answer files for unattended or remote installation

You can disable Internet Connection Sharing during workstation deployment by using standard methods for unattended or remote installation. In the [Homenet] section of the answer file, you can place entries for installing home networking settings for network adapters, Internet Connection Sharing, and Internet Connection Firewall. For Internet Connection Firewall you can specify the adapters for which ICF must be turned on. To disable Internet Connection Sharing using an answer file, the entry is as follows:

```
[Homenet]
EnableICS = No
```

For more information about unattended and remote installation, see Appendix A, "Resources for learning about automated installation and deployment."

Using Group Policy

Group Policy settings for disabling ICS and ICF in a large organizational network are described as follows:

- **Prohibit Use of Internet Connection Sharing on your DNS domain network**

  This policy setting determines whether administrators can enable and configure the Internet Connection Sharing (ICS) feature on a connection. It also determines if ICS can run on a computer when the computer is connected to the DNS domain in which the policy setting is applied.

- **Prohibit Use of Internet Connection Firewall on your DNS domain network**

This policy setting determines whether administrators can enable and configure the Internet Connection Firewall feature on a connection. It also determines if ICF can run on a computer when the computer is connected to the DNS domain in which the policy setting is applied.

Important These policy settings are location-aware. They apply only when a computer is connected to the same DNS domain network it was connected to when the policy setting was refreshed on that computer. If a computer is connected to a DNS domain network other than the one it was connected to when the policy setting was refreshed, the policy setting does not apply.

These policy settings are located in Computer Configuration\Administrative Templates\Network\Network Connections. Configuration options are described in the following table.

Group Policy settings for controlling Internet Connection Sharing and Internet Connection Firewall

Policy setting	**Description**
Prohibit Use of Internet Connection Sharing on your DNS domain network (enabled)	If you enable this policy setting, ICS cannot be enabled or configured by administrators, and the ICS service cannot run on the computer. The Advanced tab in the Properties dialog box for a local area network (LAN) or remote access connection is removed. The Internet Connection Sharing page is removed from the New Connection Wizard.
Prohibit Use of Internet Connection Sharing on your DNS domain network (disabled or not configured)	If you disable this policy setting or do not configure it and have two or more connections, administrators can enable ICS. The Advanced tab in the Properties dialog box for a LAN or remote access connection is available. In addition, the user is presented with the option to enable Internet Connection Sharing in the Network Setup Wizard and Make New Connection Wizard. (The Network Setup Wizard is available only in Windows XP Professional.)
Prohibit Use of Internet Connection Firewall on your DNS domain network (enabled)	If you enable this policy setting, Internet Connection Firewall cannot be enabled or configured by users (including administrators), and the Internet Connection Firewall service cannot run on the computer. The option to enable the Internet Connection Firewall through the Advanced tab is removed. In addition, the Internet Connection Firewall is not enabled for remote access connections created through the Make New Connection Wizard.
Prohibit Use of Internet Connection Firewall on your DNS domain network (disabled or not configured)	If you disable this policy setting or do not configure it, the Internet Connection Firewall is disabled when a LAN connection or virtual private network (VPN) connection is created, but users can use the Advanced tab in the connection properties to enable it. The Internet Connection Firewall is enabled by default on the connection for which Internet Connection Sharing is enabled. In addition, remote access connections created through the Make New Connection Wizard have the Internet Connection Firewall enabled.

For more information on Internet Connection Sharing and Internet Connection Firewall, see Help and Support Center in Windows XP.

Appendix F: Add Network Place Wizard

In Microsoft Windows XP Professional Service Pack 1 (SP1) users can use the Add Network Place Wizard to create shortcuts to shared folders and resources on the network or on Web or File Transfer Protocol (FTP) servers. If users don’t have folders on a Web server already, the Add Network Place Wizard helps them create a new folder for storing files online.

The content in this appendix includes the following:

- An overview of Add Network Place
- How to control the use of Add Network Place

Overview: Add Network Place Wizard

The Add Network Place Wizard is enabled by default for all users. Users access the wizard through Control Panel\Network Connections\My Network Places\Network Tasks.

Users can use the wizard to sign up for a service that offers online storage space. They can use the space to store, organize, and share documents and pictures using a Web browser and an Internet connection. Users can also use the wizard to create a shortcut to a Web site, an FTP site, or other local network connection. To add a shortcut in My Network Places to a folder on a Web server, the Web server must support network places. Network places requires the Web Extender Client (WEC) protocol and FrontPage extensions, or the Web Distributed Authoring and Versioning (WebDAV) protocol and Internet Information Services (IIS). The user must also have read and write access to the Web server.

In a highly managed network environment administrators might want to prevent users from storing or accessing folders on a Web server. You can remove access to the Add Network Place Wizard using Group Policy.

For more information about the WEC and WebDAV protocols, see Help and Support Center.

Controlling the use of Add Network Place Wizard

You can block users from accessing the Add Network Place Wizard in My Network Places by configuring a Group Policy setting.

Configure the following Group Policy setting in User Configuration\Administrative Templates\Windows Components\Windows Explorer: **Remove "Map Network Drive" and "Disconnect Network Drive**."

When you enable this policy setting, in addition to preventing users from using Windows Explorer or My Network Places to map or disconnect network drives, you also remove the Add a network place option from My Network Places. Users can still connect to another computer on your intranet by typing the name of a shared folder in the Run dialog box.

Note This policy setting was documented incorrectly on the Explain tab in Group Policy for Windows 2000. The Explain tab states incorrectly that this policy setting prevents users from connecting and disconnecting drives.

Appendix G: New Connection Wizard

In Microsoft Windows XP Professional Service Pack 1 (SP1) you use New Connection Wizard to create Internet and other types of network connections for home and small office networks. While this feature is designed for home and small office use, information about this feature is presented here so IT administrators can be aware of these potential capabilities within your organization's network.

The content in this appendix includes the following:

- An overview of New Connection Wizard
- How to control the use of New Connection Wizard

Overview: New Connection Wizard

New Connection Wizard in Windows XP SP1 replaces the Windows 2000 Network Connection Wizard and Internet Connection Wizard. Administrators for a home or small office network can use the New Connection Wizard to create any type of network connection including Internet, incoming, dial-up, virtual private network (VPN), and direct connection.

Administrators can create a new connection through Control Panel\Network Connections. When you click **Create a new connection**, the wizard guides you through this process. In a highly managed network environment you might want to prevent administrators as well as users from creating new connections.

Controlling the use of New Connection Wizard

You can block administrators and users from using New Connection Wizard by configuring Group Policy. Use the following Group Policy settings in User Configuration\Administrative Templates\Network\Network Connections to prevent administrators and users from using New Connection Wizard:

- **Prohibit Access to New Connection Wizard**

  The policy setting determines whether users, including administrators, can use the New Connection Wizard, which creates new connections.

  Important If the policy setting **Enable Windows 2000 Network Connections settings for Administrators** is disabled or not configured, **Prohibit Access to New Connection Wizard** will not apply to administrators on computers running Windows XP.

- **Enable Windows 2000 Network Connections settings for Administrators**

  This policy setting determines whether policy settings that exist in Windows 2000 will apply to administrators. The set of Network Connections policy settings that exist in Windows 2000 also exists in Windows XP. In Windows 2000, all of these policy settings have the ability to prohibit the use of certain features by administrators. By default, Network Connections policy settings in Windows XP do not have the ability to prohibit the use of features from administrators.

  Note This policy setting is intended to be used in a situation in which the Group Policy object (GPO) contains computers running both Windows 2000 and Windows XP and identical Network Connections policy setting behavior is required between those computers.

Configuration options for these policy settings are presented in the following table.

Group Policy settings for controlling the use of New Connection Wizard

Policy setting	Description
Prohibit Access to the New Connection Wizard (enabled)	If you enable this policy setting (and enable the **Enable Network Connections settings for Administrators** policy setting), the Make New Connection icon does not appear in the Start Menu or in the Network Connections folder. As a result, users (including administrators) cannot start the New Connection Wizard.
Prohibit Access to the New Connection Wizard (disabled or not configured)	If you disable this policy setting or do not configure it, the Make New Connection icon appears in the Start menu and in the Network Connections folder for all users (except in a workgroup environment where only administrators can access this wizard). Clicking the Make New Connection icon starts the New Connection Wizard. Changing this policy setting from enabled to not configured does not restore the Make New Connection icon until the user logs off or on. When other changes to this policy setting are applied, the icon does not appear or disappear in the Network Connections folder until the folder is refreshed.
Enable Windows 2000 Network Connections settings for Administrators (enabled)	If you enable this policy setting, the Windows XP policy settings that existed in Windows 2000 will have the ability to prohibit administrators from using certain features (see Network Connections policy settings). With this policy setting enabled, policy settings that exist in both Windows 2000 and Windows XP behave the same for administrators.
Enable Windows 2000 Network Connections settings for Administrators (disabled or not configured)	If you disable this policy setting or do not configure it, Windows XP policy settings that existed in Windows 2000 will not apply to administrators.

For information about using the Group Policy Object Editor, see Appendix B, "Resources for learning about Group Policy."

Related Links

This section contains a list of the Web sites found in other sections of this white paper.

Links to product information, support information, TechNet, Microsoft Developer Network, and information in resource kits

The following sites provide information about Windows XP and other Microsoft products. The list includes sites containing product Help as well as other basic sites that provide information about Microsoft operating systems and other Microsoft products:

- Windows XP:

  www.microsoft.com/windowsxp/

- Windows 2000 Help on the Web, including Help for servers running Windows 2000 (Appendix A, "Resources for learning about automated installation and deployment," provides links to specific topics in Help):

  www.microsoft.com/windows2000/techinfo/proddoc/

- Windows Catalog:

  www.microsoft.com/windows/catalog/

- Microsoft Product Support Services:

  support.microsoft.com/

- Microsoft TechNet:

  www.microsoft.com/technet/

- Microsoft Developer Network:

  msdn.microsoft.com/

- Prescriptive Architecture Guides:

  www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/idc/pag/pag.asp

- Windows Deployment and Resource Kits:

  www.microsoft.com/reskit/

- Windows 2000 Server Resource Kit, Supplement 1:

  www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp

- Internet Explorer Administration Kit:

  www.microsoft.com/windows/ieak/

- NetMeeting 3 Resource Kit (the NetMeeting section in this white paper provides links to specific chapters in this kit):

  - www.microsoft.com/technet/prodtechnol/netmting/reskit/netmtg3/cover.asp
  - www.microsoft.com/windows/NetMeeting/Corp/ResKit/

Links to information about security, management, and deployment

The following sites provide information about security, management, and deployment topics:

- Managing mobile code:

  www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bestprac/mblcode.asp
- Best practices for enterprise security:

  www.microsoft.com/technet/security/bestprac/bpent/bpentsec.asp
- Deploying Windows XP:

  www.microsoft.com/windowsxp/pro/techinfo/deployment/planning/default.asp
- Automated installation and deployment:
  - Automating and customizing installations:

    www.microsoft.com/technet/prodtechnol/winxppro/reskit/prbc_cai_nmip.asp
  - Automating server installation and upgrade:

    www.microsoft.com/windows2000/techinfo/reskit/en-us/deploy/dgcb_ins_adeb.asp
  - Systems Management Server as a deployment tool:

    www.microsoft.com/windows2000/techinfo/reskit/en-us/deploy/dggf_sms_zunm.asp

Links to information about components in Windows XP Professional SP1 or tools you can use with Windows XP Professional SP1

The following sites provide information about some of the components in Windows XP Professional SP1:

- Application Help:

  www.microsoft.com/windowsxp/appexperience/default.asp
- Certificates, certificate status, and certificate revocation:

  www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/WinXPPro/support/tshtcrl.asp
- Driver Protection:

  www.microsoft.com/hwdev/driver/drv_protect.asp
- Dynamic Update:

  www.download.windowsupdate.com/msdownload/update/v3/static/DUProcedure/Dynamic Update.htm
- Help and Support Center Headlines (for an explanation of how Headlines and the Newsver.xml file work, see "Help and Support Center: The Headlines and Online Search features" earlier in this white paper):

  windows.microsoft.com/windowsxp/newsver.xml
- Internet Explorer:

  www.microsoft.com/windows/ie/

For additional information about Internet Explorer, see "Internet Explorer Administration Kit" in "Links to product information, support information, TechNet, and information in resource kits" earlier in this section.

- Internet Explorer and File association Web service, language codes (relates to registry settings used for specifying language):

  msdn.microsoft.com/library/default.asp?url=/library/en-us/wceielng/htm/cooriMLangRegistrySettings.asp

- Internet games:
  - www.zone.msn.com/hub_flog.asp
  - www.zone.msn.com
- Internet Information Services:
  - www.microsoft.com/technet/security/prodtech/windows/iis/default.asp
  - www.microsoft.com/WindowsXP/pro/evaluation/overviews/iis.asp
- Internet Protocol version 6:

  www.microsoft.com/windowsserver2003/technologies/ipv6/

- MSN Explorer (specifically, the MSN.com Web site):

  privacy.msn.com/

- NetMeeting:
  - www.microsoft.com/windows/NetMeeting/
  - www.microsoft.com/technet/prodtechnol/netmting/evaluate/nm3feats.asp
  - support.microsoft.com/default.aspx?scid=KB;en-us;Q158623
  - support.microsoft.com/default.aspx?scid=/support/netmeeting/howto/default.asp

  For additional information about NetMeeting, see "NetMeeting 3 Resource Kit" in "Links to product information, support information, TechNet, and information in resource kits" earlier in this section.

- Remote Assistance:

  support.microsoft.com/default.aspx?scid=kb;en-us;300692

- Search Companion:

  sa.windows.com/privacy/

- Windows Error Reporting:
  - watson.microsoft.com/dw/1033/dcp.asp
  - msdn.microsoft.com/library/default.asp?url=/library/en-us/debug/base/windows_error_reporting.asp
  - oca.microsoft.com/en/cerintro.asp
- Windows Media Player:
  - www.microsoft.com/Windows/WindowsMedia/
  - windowsmedia.com/privacy/privacystatement.asp
  - www.microsoft.com/windows/windowsmedia/software/v8/privacy.asp

- Windows Messenger:
  - messenger.microsoft.com/support/privacypolicy.asp
  - www.microsoft.com/exchange/techinfo/administration/2000/ClientKeys.asp
  - www.microsoft.com/windowsxp/pro/techinfo/deployment/natfw/default.asp
- Windows Time service:
  - www.microsoft.com/windows2000/techinfo/howitworks/security/wintimeserv.asp
  - www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/maintain/operate/wintime.asp
  - support.microsoft.com/default.aspx?scid=kb;en-us;Q223184
- Windows Update:
  - windowsupdate.microsoft.com/
  - corporate.windowsupdate.microsoft.com
  - www.microsoft.com/windows2000/windowsupdate/sus/default.asp

The following site provides information about using tools that work with Windows XP Professional SP1:

- Windows Application Compatibility Toolkit:

  www.microsoft.com/windowsxp/appexperience/

Links to information about licensing, product activation, and registration

The following sites provide information about licensing, product activation, and registration:

- www.microsoft.com/licensing/
- www.microsoft.com/licensing/resources/vol/volkeys_winxpsp1.asp
- www.microsoft.com/piracy/basics/activation/
- www.microsoft.com/piracy/basics/activation/apolicy.asp
- www.microsoft.com/piracy/basics/activation/windowsxpsp1.asp
- www.microsoft.com/piracy/basics/activation/prvcyms.asp

Links to sites maintained by task forces and other organizations

The following sites are maintained by the Internet Engineering Task Force:

- www.ietf.org/html.charters/ngtrans-charter.html
- www.ietf.org/rfc/rfc1510.txt
- www.ietf.org/rfc/rfc2373.txt?number=2373/
- www.ietf.org/rfc/rfc3056.txt?number=3056/

(Web addresses can change, so you might be unable to connect to the Web site or sites mentioned here.)

The following sites are maintained by the International Multimedia Telecommunications Consortium:

- www.imtc.org/
- www.imtc.org/h323.htm

(Web addresses can change, so you might be unable to connect to the Web site or sites mentioned here.)

The following site is maintained by the International Telecommunication Union:

- www.itu.int/home/index.html/

(Web addresses can change, so you might be unable to connect to the Web site or sites mentioned here.)

Links to information about Group Policy

The following sites provide information about topics related to Group Policy:

- Resource Kit Group Policy reference:

  www.microsoft.com/windows2000/techinfo/reskit/en-us/w2rkbook/gp.asp
- Group Policy Object settings spreadsheet:

  www.microsoft.com/WindowsXP/pro/techinfo/productdoc/gpss.asp
- Using Group Policy to manage desktops:

  www.microsoft.com/technet/prodtechnol/winxppro/reskit/prda_dcm_jplq.asp
- Managing Windows XP in a Windows 2000 server environment:

  www.microsoft.com/windowsxp/pro/techinfo/administration/policy/default.asp
- Implementing Registry-Based Group Policy:

  www.microsoft.com/windows2000/techinfo/howitworks/management/rbppaper.asp